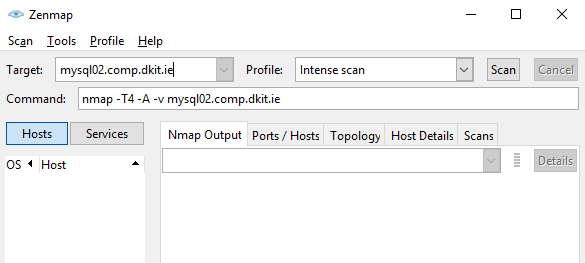
**Application Security CA2**

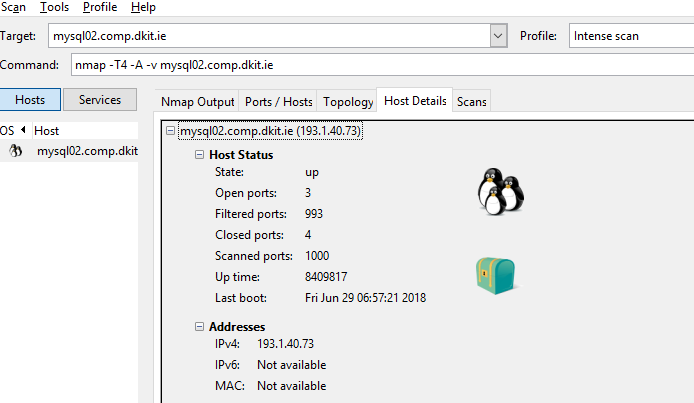
1. **2. 3. 4. 5. 6.**

Target mysql02.comp.dkit.ie

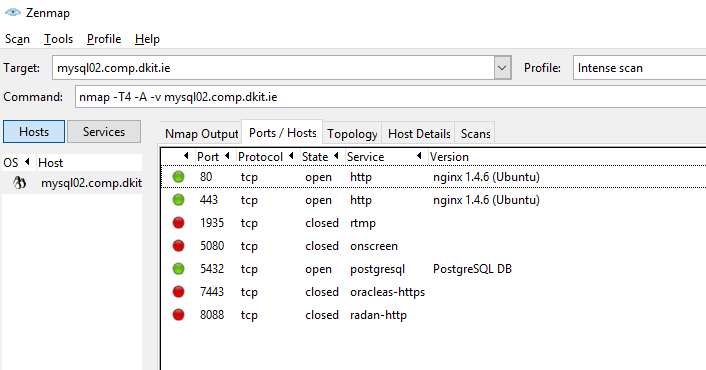
The above address has been entered into the target field on Zenmap, the profile is set to intense scan and the scan button is clicked.



1. The IP address of mysql02.comp.dkit.ie is 193.1.140.73 this is a public IP address.



1. The open ports on the server are port 80, 443 and 5432



1. By default the port number for a web server is 80, it’s the port that the server listens on for incoming requests from any web client.

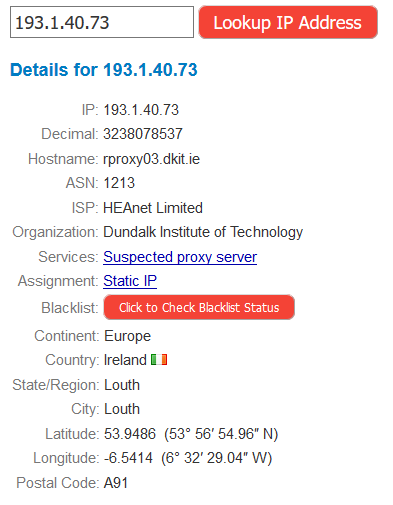
Web Servers listen on port 443 for incoming requests from web clients, it differs from port 80 because it utilises secure web browser communication with the SSL handshake using the http service and public key encryption.

Port 5432 is the default port used by PostgreSQL database server to listen for connections from client apps.

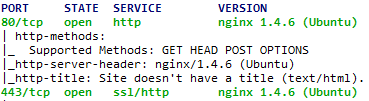
1. The name of the server that has been scanned rproxy03.dkit.ie with an IP address 193.1.40.73

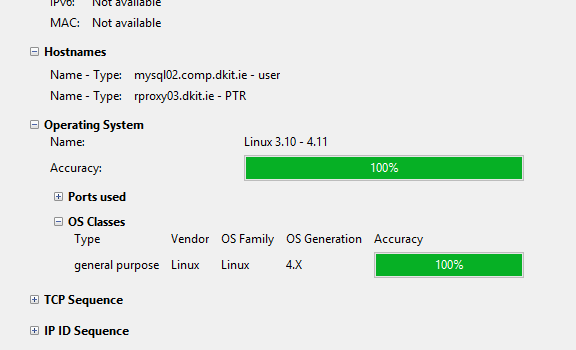


1. Its services are a suspected proxy server

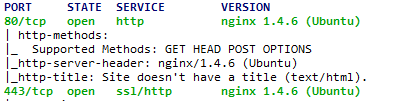


1. The operating system running the server is Linux and the OS is nginx/1.4.6 Ubuntu.

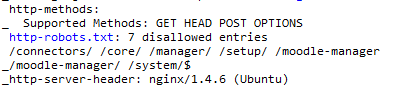




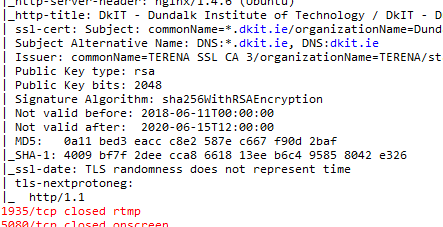
1. Get, Head and Post methods are supported by the server



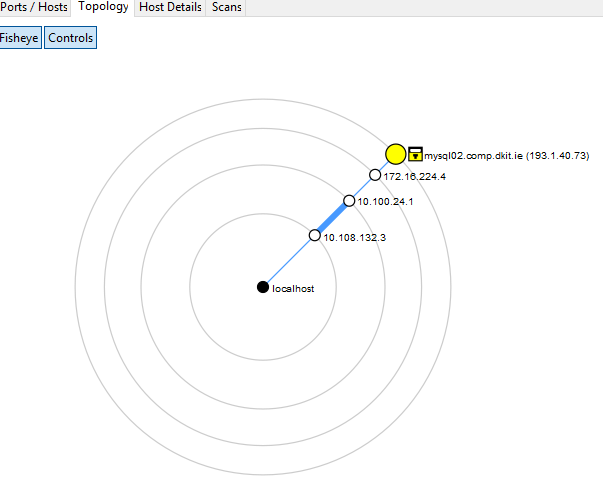
1. There are 7 disallowed entries of the robots.txt file



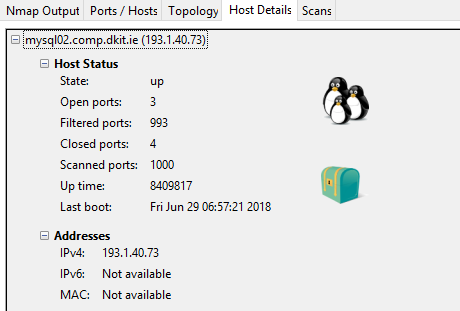
1. Terena in Holland signs the certificates 11 june 2018 15 june 2020



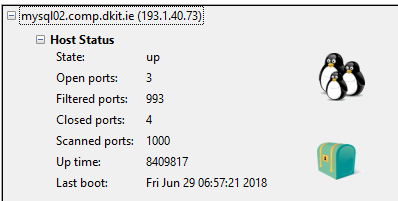
1. There are three network services between the localhost and the server.



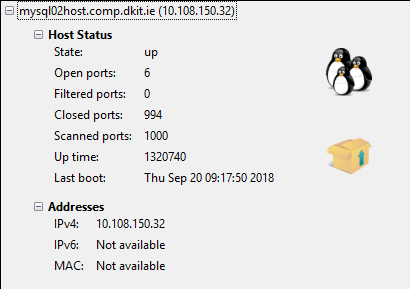
1. 993 ports are filtered on the server.



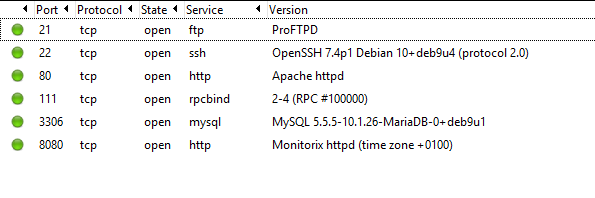
1. The server was last rebooted on the 29th of June 2018 at 06.57.21



1. **(6)** The IP address of mysql02host.comp.dkit.ieon display is 10.108.150.32. this is a private IP address making the servers actual IP address hidden. Routers generally use these IP addresses to assign to local computers. The numbers generally represent computers on an internal network.



There are 6 open ports on the server, port 21, 22, 80, 111, 3306 and 8080.



Port 21 is the file transfer protocol, where servers listen for incoming client connections.

Port 22 uses secure shell to manage network devices securely at the command level.

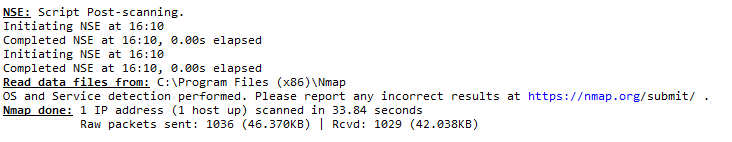
Port 80 is the default port a server listens on for incoming requests from any web client.

Port 111 provides information between Unix based systems, it provides a directory or mapping between available services and their ports.

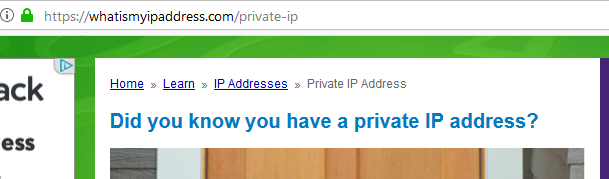
Port 3306 uses the transmission control protocol, data is always delivered the same way it was sent unlike UDP.

Port 8080 is a place to host a secondary web server over port 80. It’s used for proxy and caching.

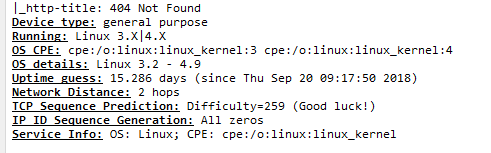
**(7)** There appears to be no name revealed for the server. The rDNS was under the NSE of the mysql02.cpm.dkit.ie but not on this scan, cannot locate it anywhere else on the scan.



**(8)** The Scan has shown that the only IP address displayed anywhere on the ZenMap scan was private.



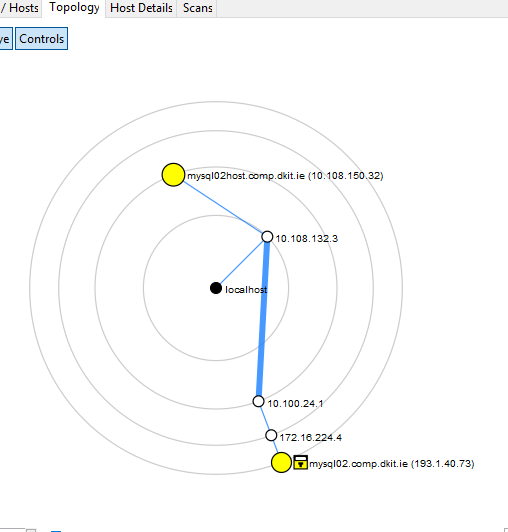
**(9)** This device is also running Linux, Ubuntu is not specified but it’s likely it or a headless version of it.



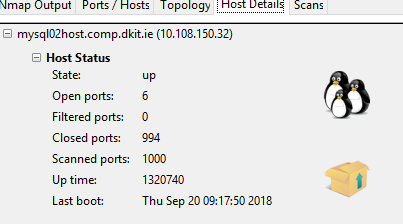
**(11)** The host does not have a robots.txt file on it, there was no evidence of it anywhere in the Nmap output.

**(12)** The host scan does not show which organisation signs the DkITs SSL certificates but its assumed to be the same as mysql02.com.dkit.ie scan previously with the same valid from and to dates.

**(13)** There are three network services between the local host and server host.



**(14)** There are 994 closed ports on the host.



**(15)** Server was last rebooted on 20th of September 2018 at 09:17:50

