Douglas McClure

3/1/2021

Pen Testing

Ping: This tests your connection to the server.

Nslookup: Gives local addresses connected to the server.

Whois: Gives the domain information.

IPBlock: whois variation used to determine the ownership and contact information for a block of

IP addresses.

Dig: Returns all DNS records associated with the server.

Traceroute: identify the network path that must be followed to reach one system from another which provides the names and IP addresses of all intermediate systems to provide potential intermediate attack points or estimate the geographic location of a server.

Finger: Obtains host/user information from a system running the finger daemon.

Time: Gives the remote or local timezone.

Blacklist: Gives the addresses from the abuse query.

Abuse Lookup: This produces also information from the abuse.net query.