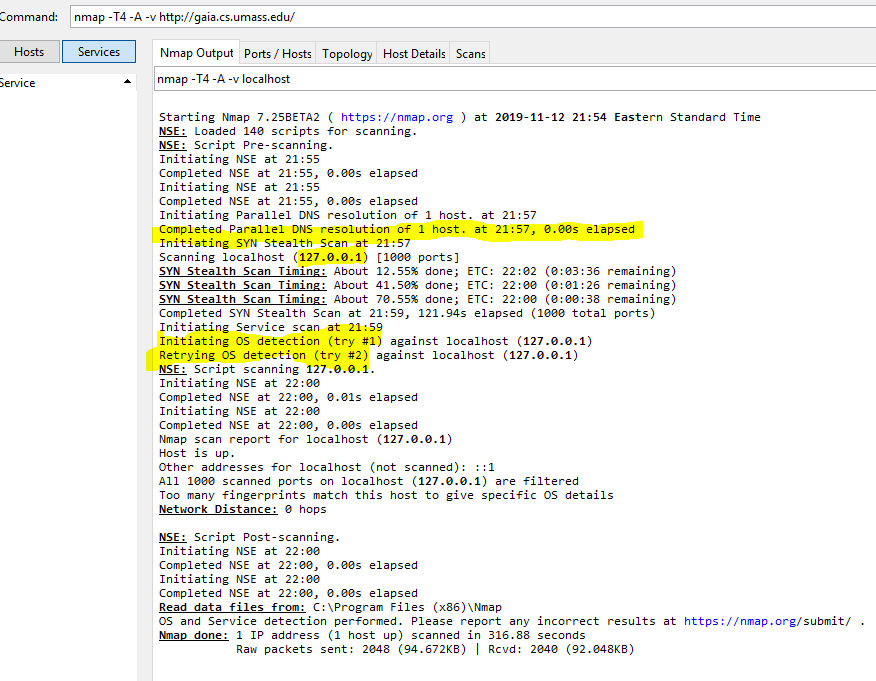
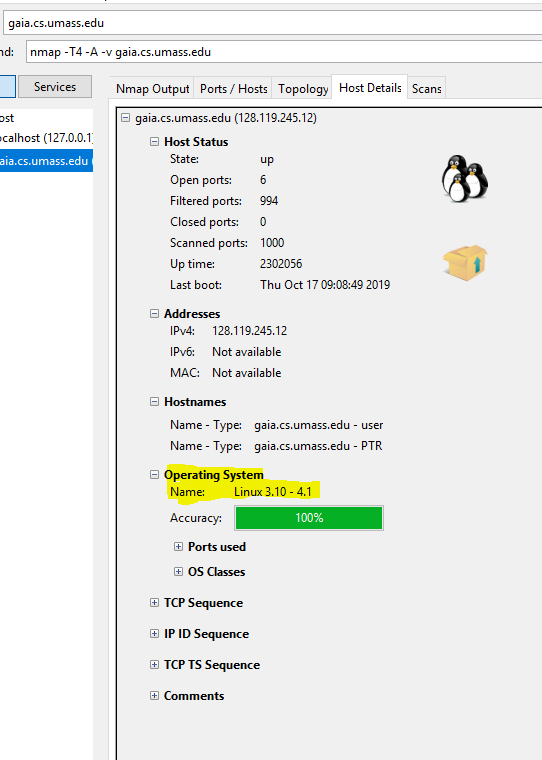
Targets = My localhost and <http://gaia.cs.umass.edu/>

1. Scan the hosts and report the Operating System (including version), the server application if any (including version), the IP address of the target host, DNS server of the target domain, open ports and services (if available) running on these ports.

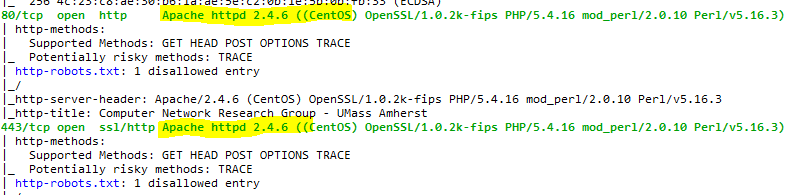
Local host results- could not fingerprint operating system. No server application. Target IP address is 127.0.0.1.No DNS resolution or ports running.



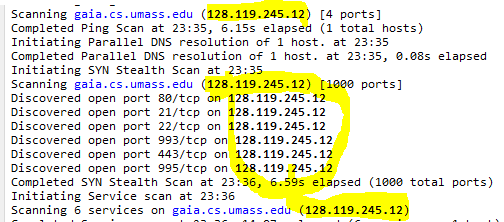
Results of Gaia – Operating system is Linux 3.10-4.1



Server application is apache 2.4.6



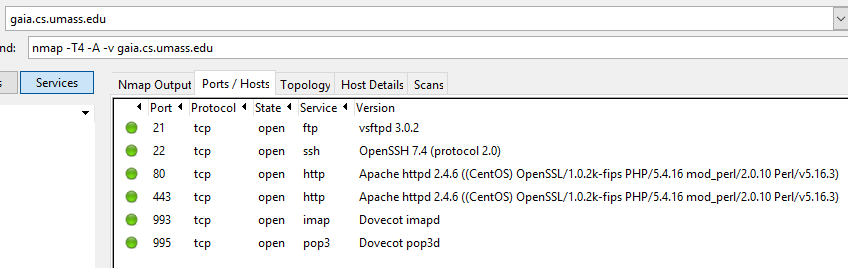
IP Address is 128.119.245.12 (Also seen above.)



No DNS server recovered.



Services are FTP, SSH, HTTP, IMAP, and POP3

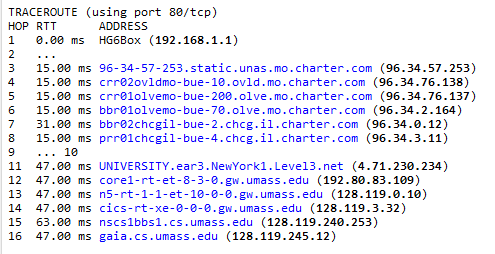


1. List any possible vulnerabilities related to the services identified in the previous step.

Some vulnerabilities with the Gaia domain is that it uses FTP, HTTP, IMAP, and POP3.These are insecure and can be replaced with their more secure counter parts such as SFTP instead of FTP, HTTPS instead of HTTP, and SMTP instead of IMAP or POP3.

1. Show the output of the traceroute program (executed within Nmap) to access http://gaia.cs.umass.edu/.

Traceroute runs through charter and level3 communications.



1. Explore additional features of the tool and demonstrate any findings you think useful.

One interesting feature that is useful with the NMAP GUI is the topology feature. This is useful when visualizing the network.



1. Based on your experience, how will you evaluate the tool? In what aspects could the tool be improved?

NMAP is a very useful tool for fingerprinting a network and seeing what services are available to be exploited. If NMAP wanted to add some extra features and functionality they could add a packet crafting feature to help test network security.