Project 1: Firewall and Access Control

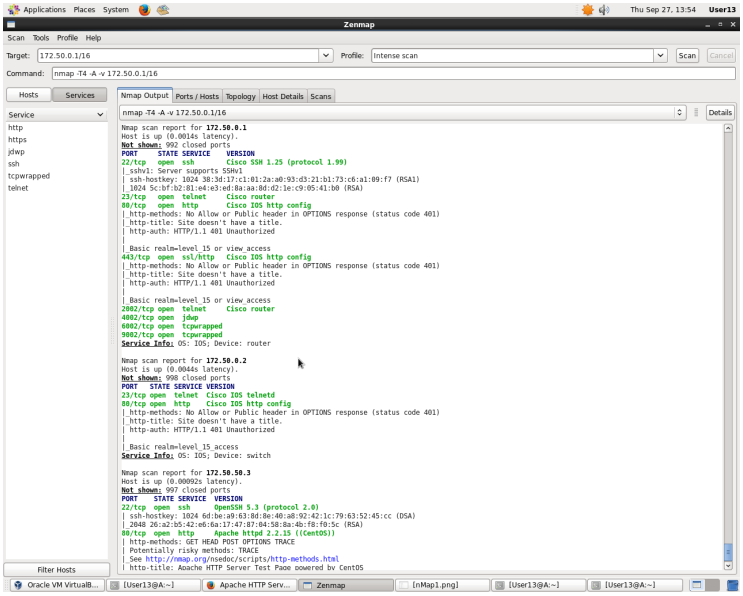
Miguel Archundia
Jacobo Sanchez
Derek Hernandez
Salvador Romero Mondragon

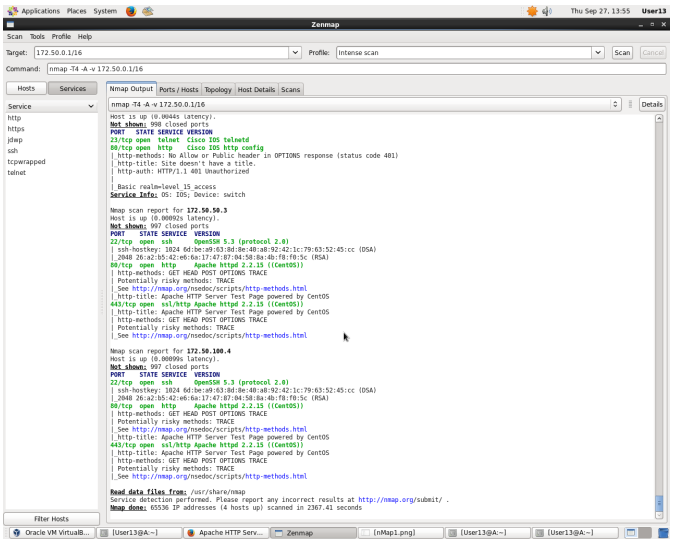
Section I

Report sections II - IV were compiled by Salvador. Access control matrix was provided by Derek. Jacob wrote section I and revised report prior to submission. Miguel assisted with screen shot gathering and insertion. Jacob and Miguel performed Task I network setup which was then verified by Salvador and Derek. Miguel performed section II with assistance from Jacob. Miguel performed Task III. Jacob and Miguel performed Task IV.

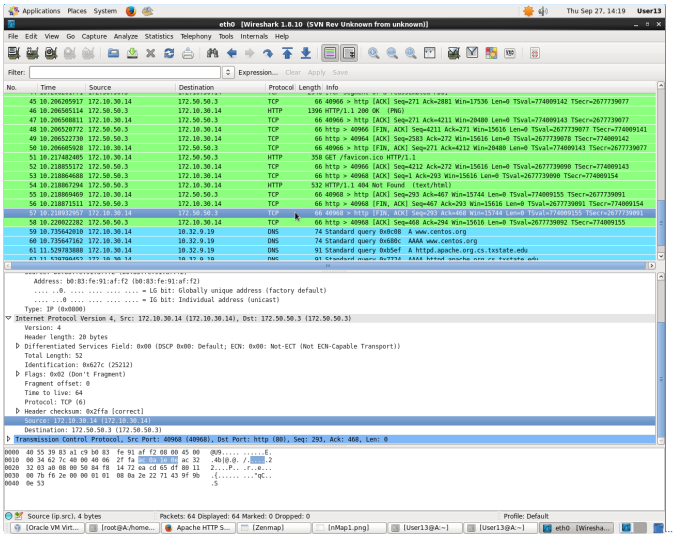
Sections II

a.)Scan showing the NMap commands to scan the computers and the service ports.



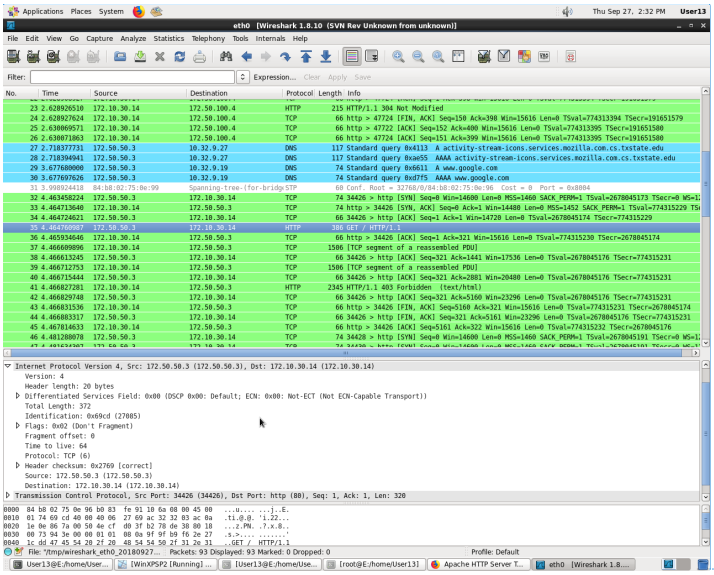


b.) Show the Wireshark screenshot of web services between computers.
A.E to E.2 Web services. Web service allowed by default.



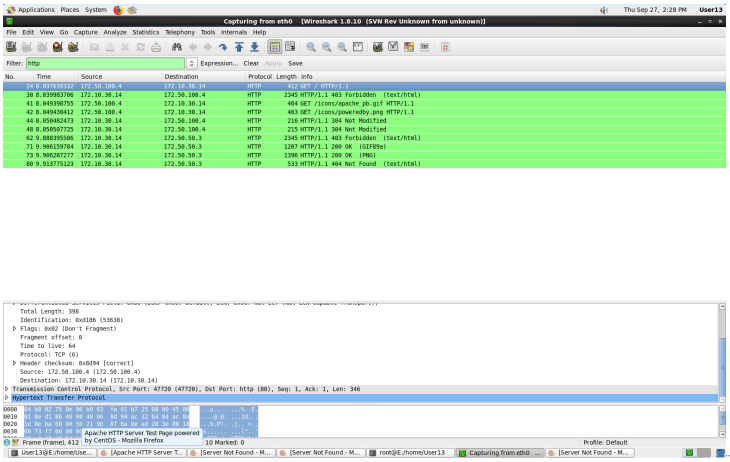
Commented [1]: A to B2 Webservices

E.1 to A.E. Web service allowed by default.



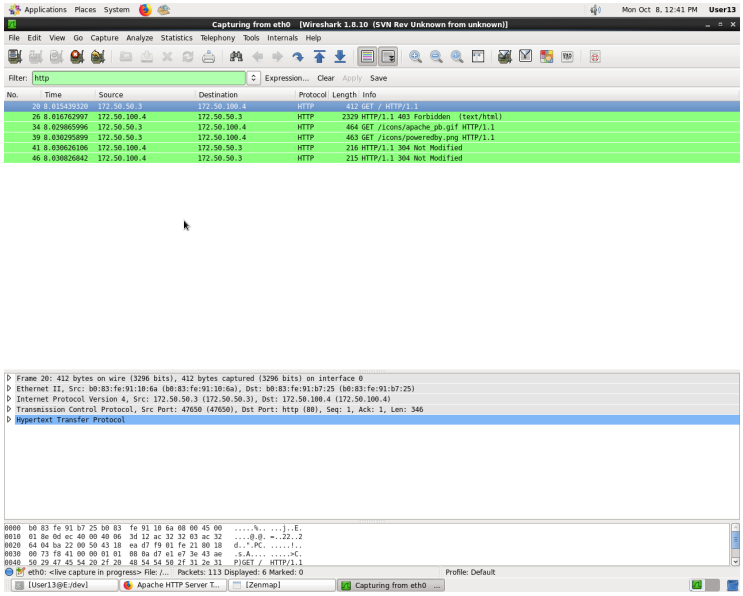
Commented [2]: B1 to A web services

E.2 to A.E Web services. Web service allowed by default.



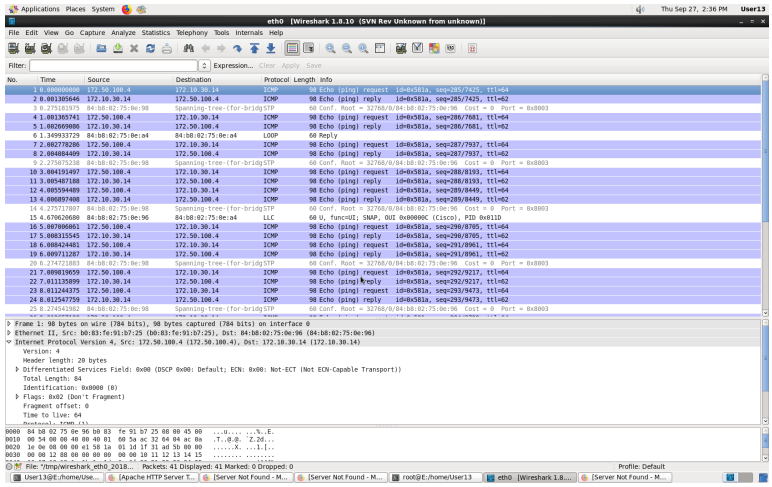
Commented [3]: B2 to A Webservices

E.1 to E.2 Web services. Web service allowed by default.



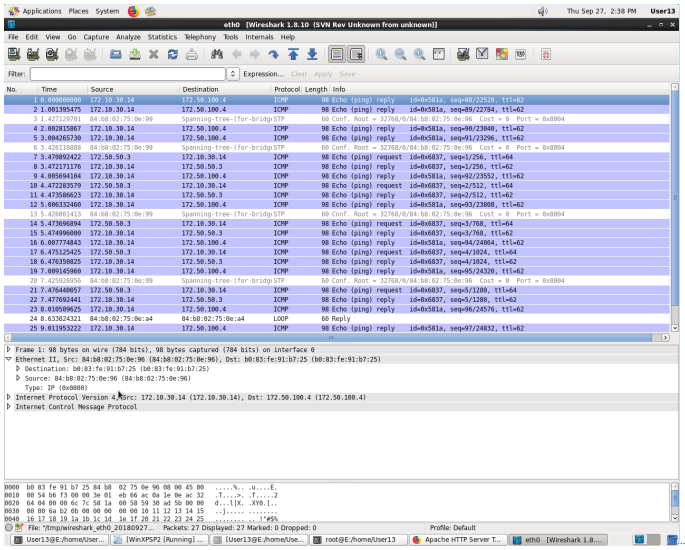
c.)Showing Ping between computers.

Ping from E.2 to A.E. Ping allowed.

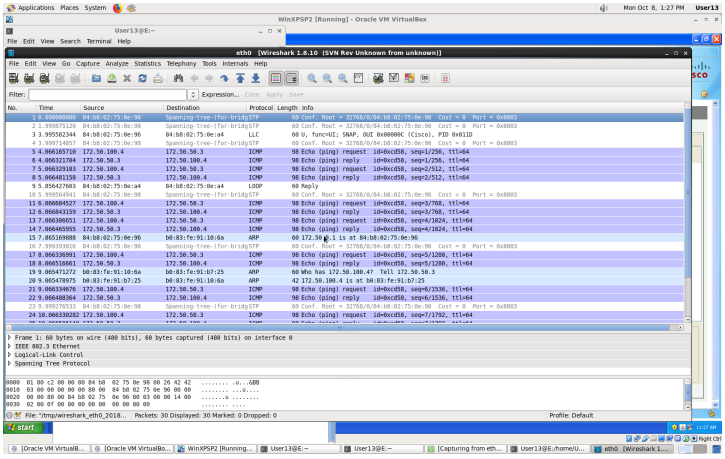


Ping E.1 to A.E. Ping allowed.

Commented [4]: B1 to A



Ping E.2 to E.1 Ping Allowed



d) The default setting for the Cisco firewall allowed both internal and external computers to give all services to the computers in the network.It implements rules sequentially and does not allow for traffic monitoring between internal computers (server to host and vice versa)

Section III

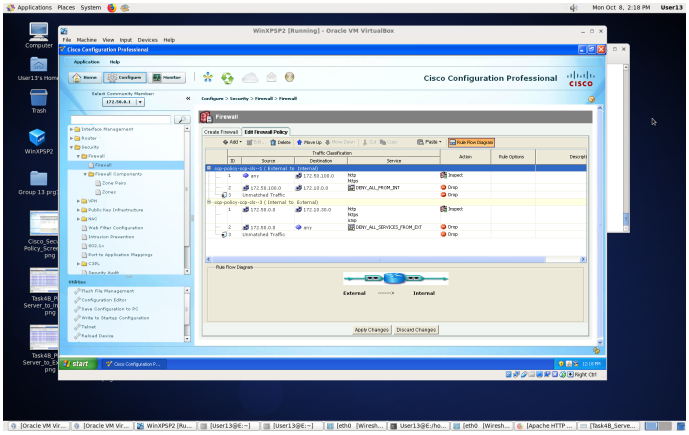
a.)Access Control Matrix

OBJECT				
SUBJECT		Internal Servers	Internal Workstation	External Computer
	Internal Server	---P	WSAP	W--P
	Internal Workstation	---P	---P	----P
	External Computer	----	W---	---P

W- Web services S- SSH A-Service Access P-Ping

b.) Rules b,partially d,e are the rules that we cannot implement using the cisco firewall and must be implemented using the iptables. Cisco software requires zone configuration. Zone source and destination cannot be the same. For rule d, iptables must be used to deny services internal to the zone. Cisco software can only be used to deny services from internal workstations to external workstations.

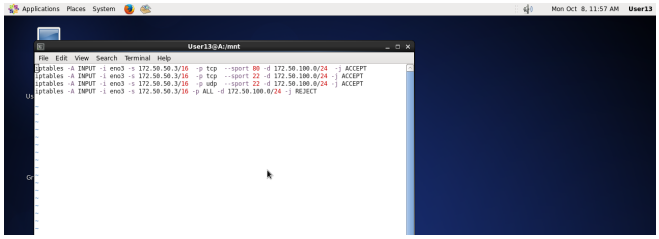
c.) Screenshot of Cisco Firewall configuration.



d.) Iptables is a packet filter that can be used in place of Cisco software. Refer to section

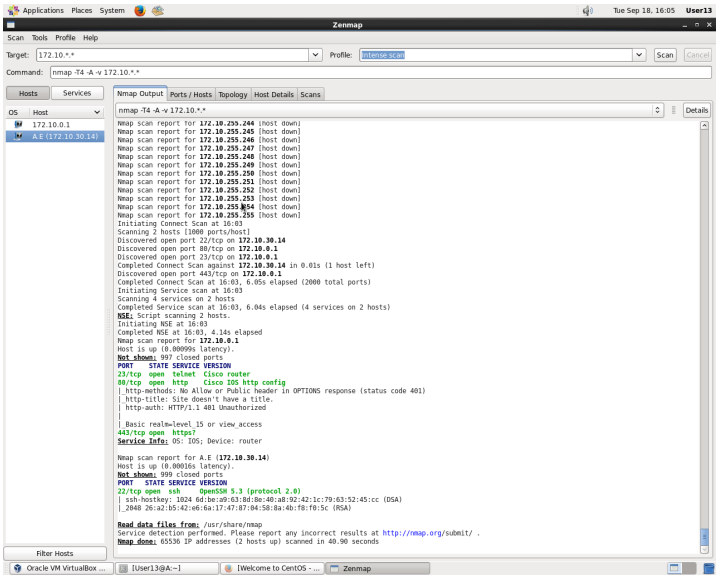
e.) below. The first line provided for web service between internal servers and internal workstations. LInes 2 and 3 provide ssh utilizing tcp and udp protocols. Line 4 rejects any service to servers. These commands are run on the server.

e.)Iptable commands in the internal server that enforce the security policy that is not implemented in the cisco firewall

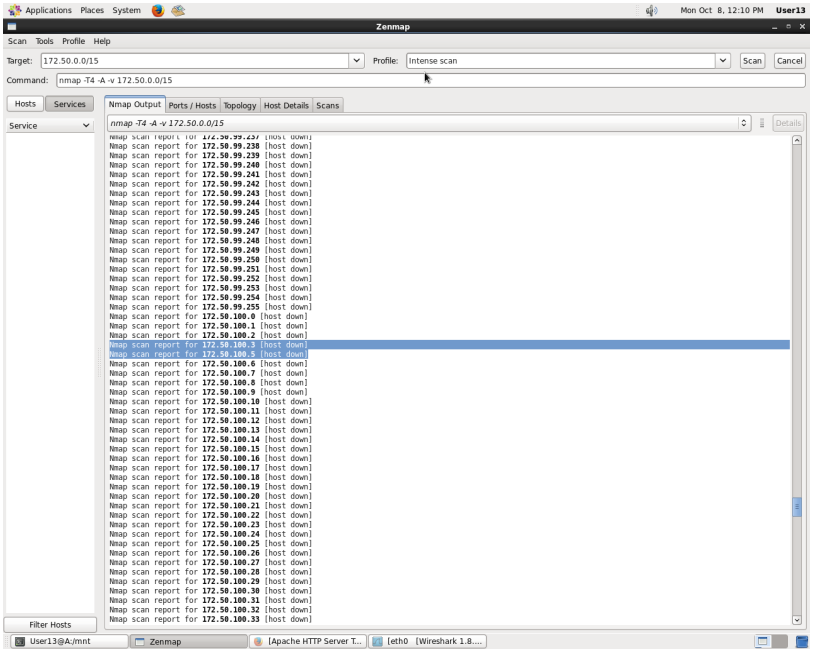


Section IV

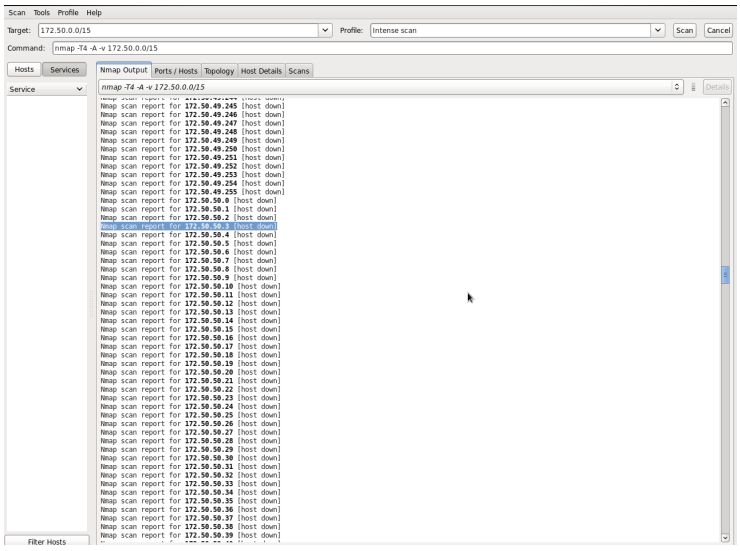
a.)Screenshot of NMap results of exposed computer and ports



Nmap of server

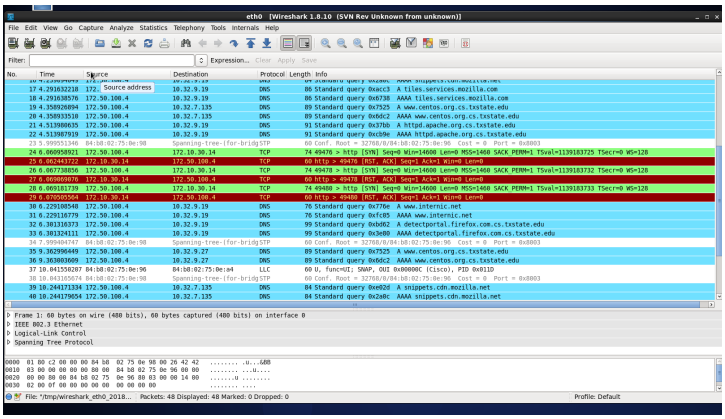


Nmap of workstation

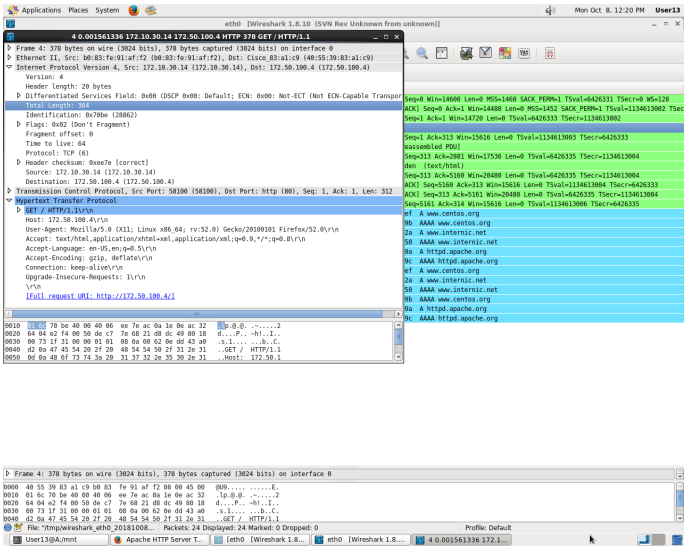


b.)Screenshot of Wireshark results of checking web services between computers

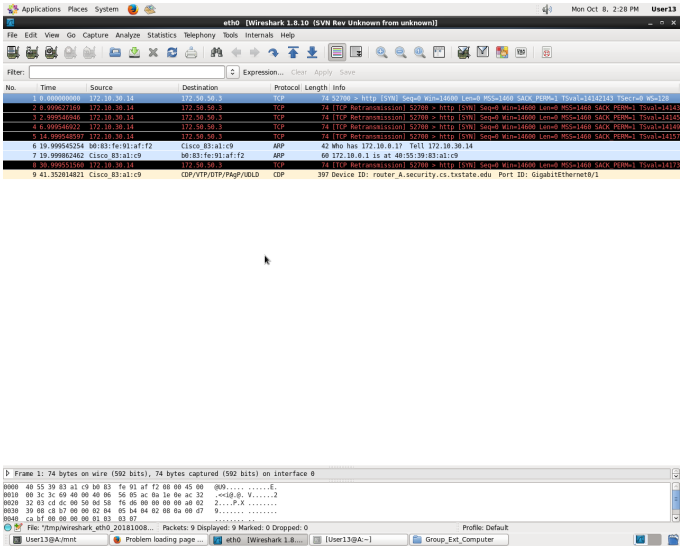
Server to External Host



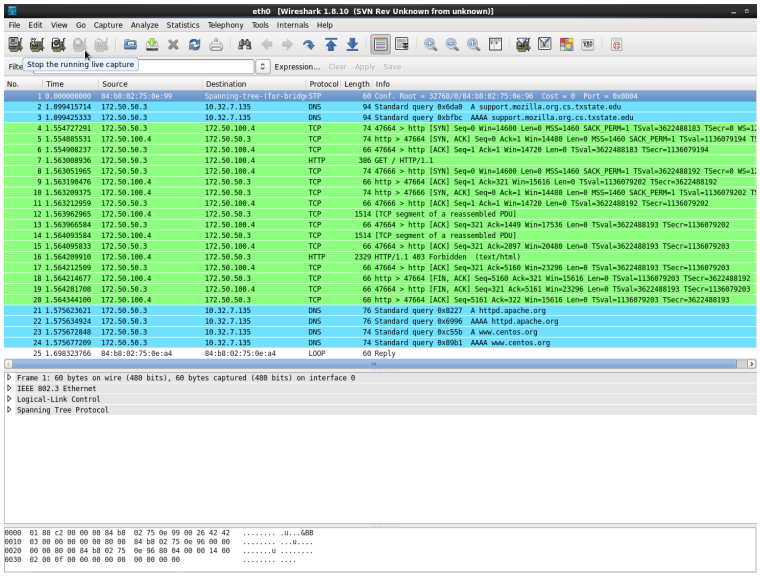
External Host to Server: Web service allowed.



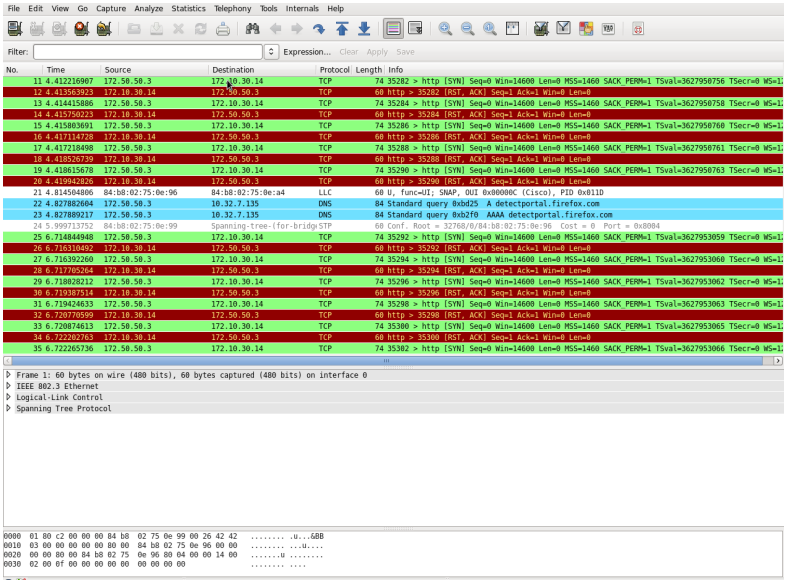
External Host to Internal workstation web service: Not allowed.



Internal Workstation to Internal Server: Web service allowed.

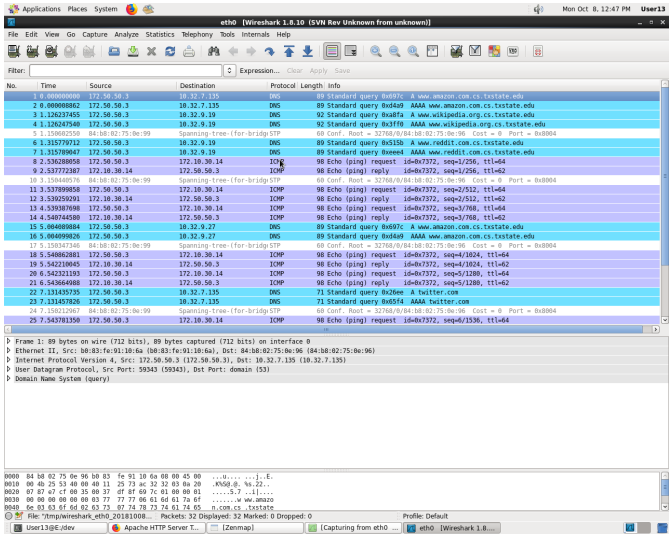


Internal workstation to external host web services not allowed, should be allowed.

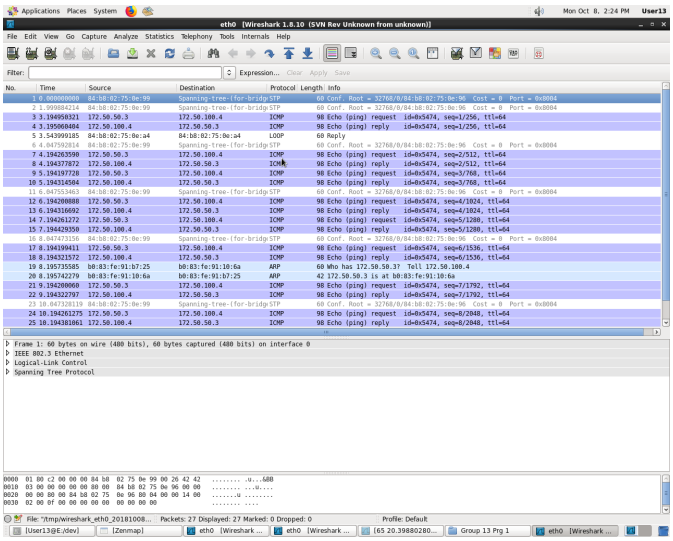


c.)Screenshot of Ping between computers(state if ping is allowed)

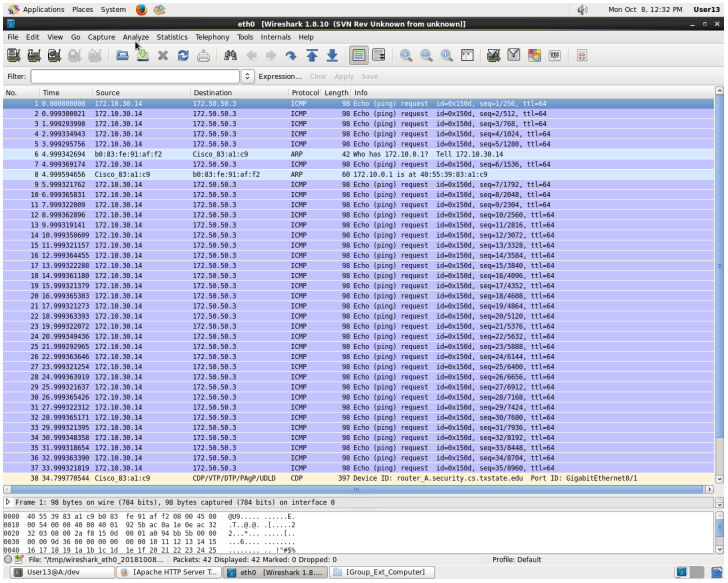
Internal Workstation to External: Ping successful



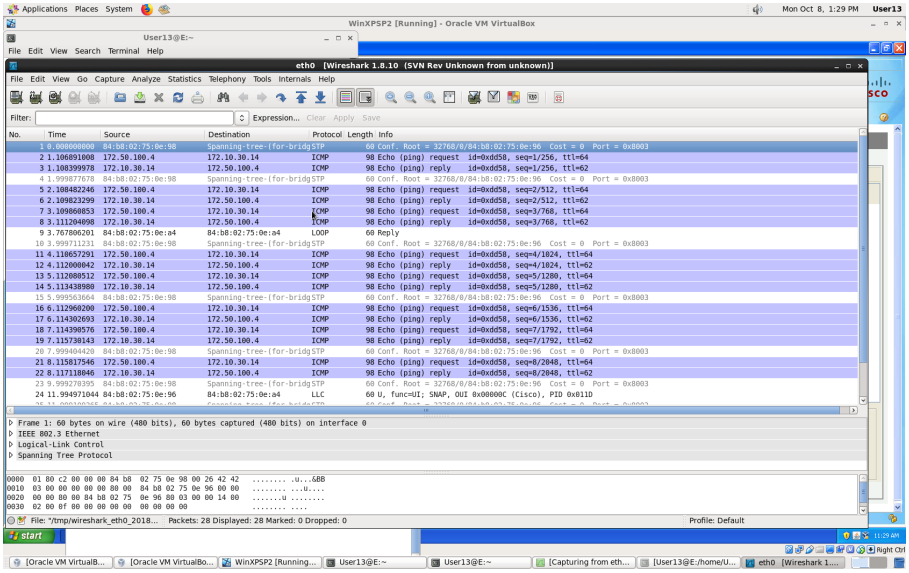
Internal Workstation to Internal Server: Ping successful



External Computer to Internal Workstation. Ping unsuccessful.



Internal Server to External Computer. Ping successful.



d.) The security policy cannot ensure that classified data will not be disclosed to the public. This is because internal workstations can access web services provided by external computers. This might expose internal computer to data breach.
There is no guarantee that the classified data can be safely stores. B.1 (E.1) is the workstations that is given SSH and Web service privileges, in a later rule the workstations is given access to services hosted by Internal Server and access to External web services. These are rules that have the potential to disclose a breach in the firewall. The breach is due to the level of classification; Internal Servers are in this scenario the highest classification while Internal workbench is second highest, and External being the lowest. The Internal workbench has access to Internal Servers Services and access to External Workbenches. The Firewall doesn't have the rules to protect data in the Internal Servers due to the versatility of Internal workbenches.