**Security Project #1**

Tyler Perkins

Christopher Ward

Matt Stanfield

Pierre Bonnain

**Section I**

For this project, we had usually two people in the lab at a time working on a task due to conflicting schedules. Task I and II were done by Tyler and Chris. Tyler and Chris were the first to come in to the lab and figure out the requirements of the project and how to set up and use the environment. Chris set up the NMap scan, while Tyler ran the tests in Wireshark for task II. Task III was done primarily by Matt and Chris. They completed the access control matrix based on the given security policy, then configured the Cisco firewall according the the matrix with some help from Tyler and Pierre. Task IV was done by Tyler and Chris. Again, Chris setup the NMap scan while Tyler ran the tests with Wireshark. Section I of this report was written by Tyler, Section II by Tyler and Chris, Section III by Matt and Pierre, and Section IV by Tyler and Chris.

**Section II**

1. NMap and Service Status Commands Used

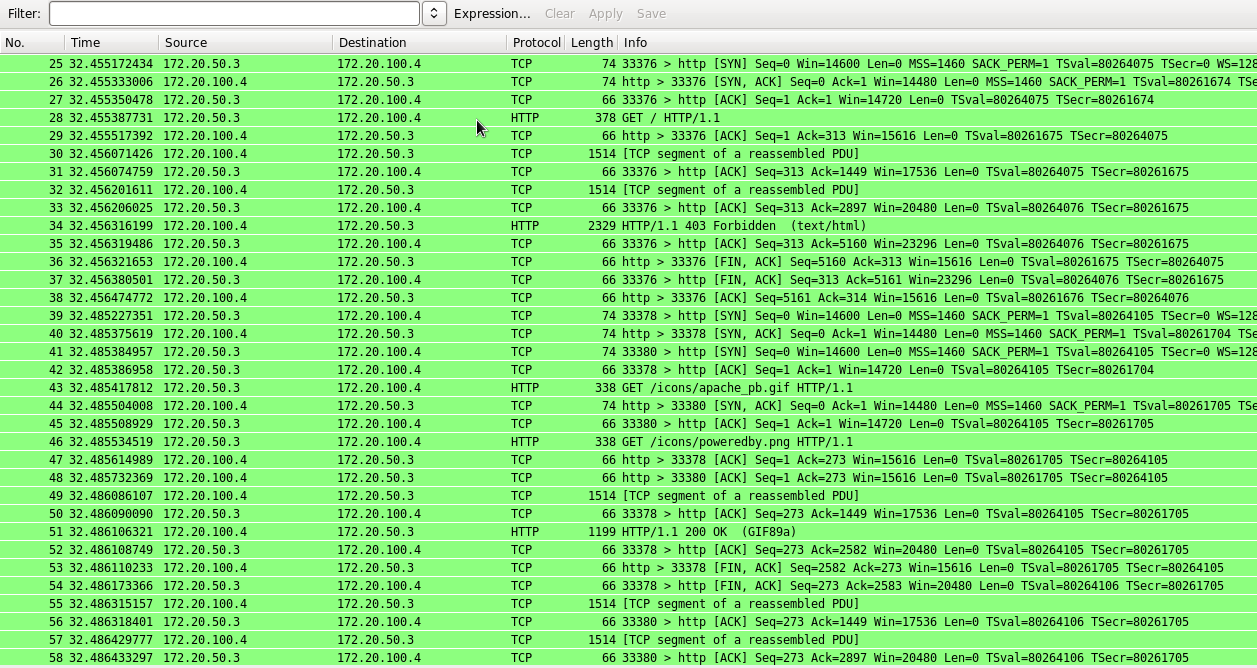
We performed the NMap Scan from computer A.B with the command:

*Nmap -T4 -A -v 172.20.01/16*

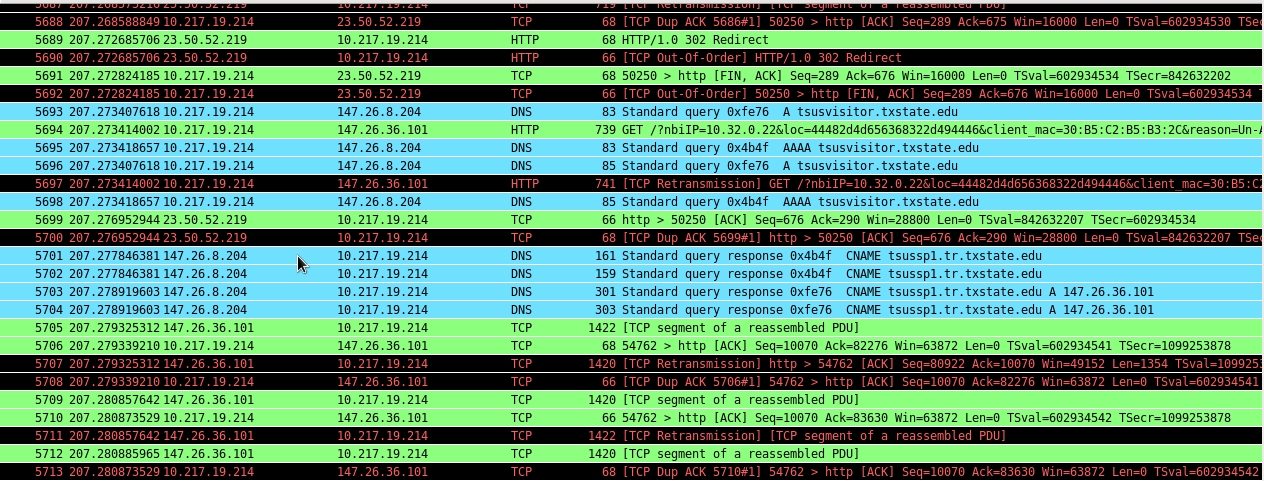
This is simply the intense scan using Network B as the target.

1. Wireshark Results for Web Services (Default Firewall)
   1. B.1 Access Web Services in B.2

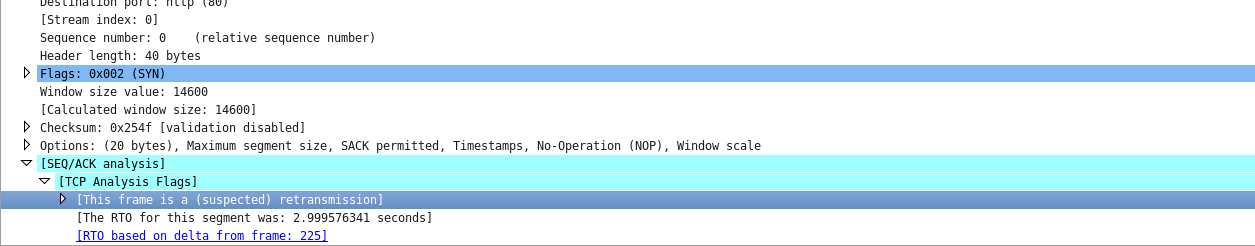
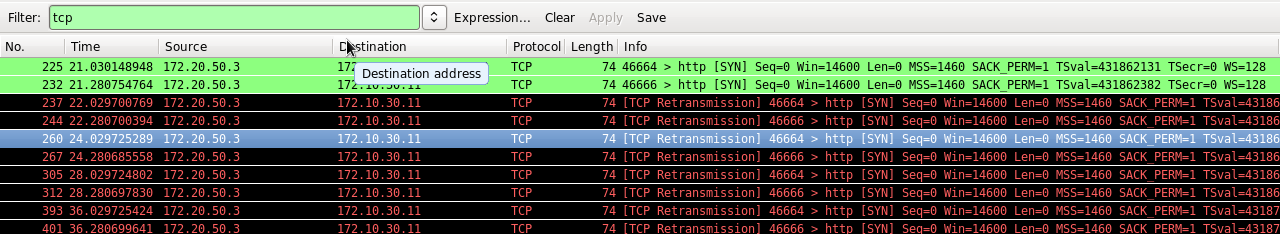
* Web service was allowed between computers.

****

* 1. A Access Web Services in B.2
* A was not able to access web services in B.2

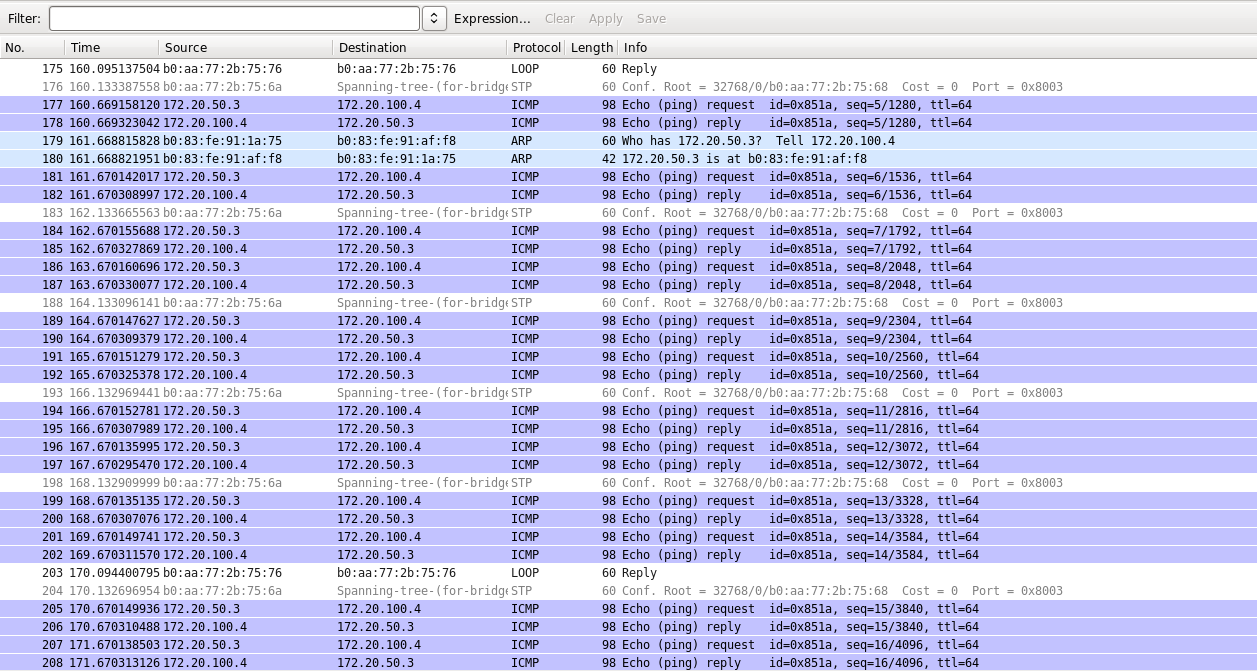


* 1. B.1 and B.2 Access Web Services in A
* B.1 and B.2 could not access web services in A

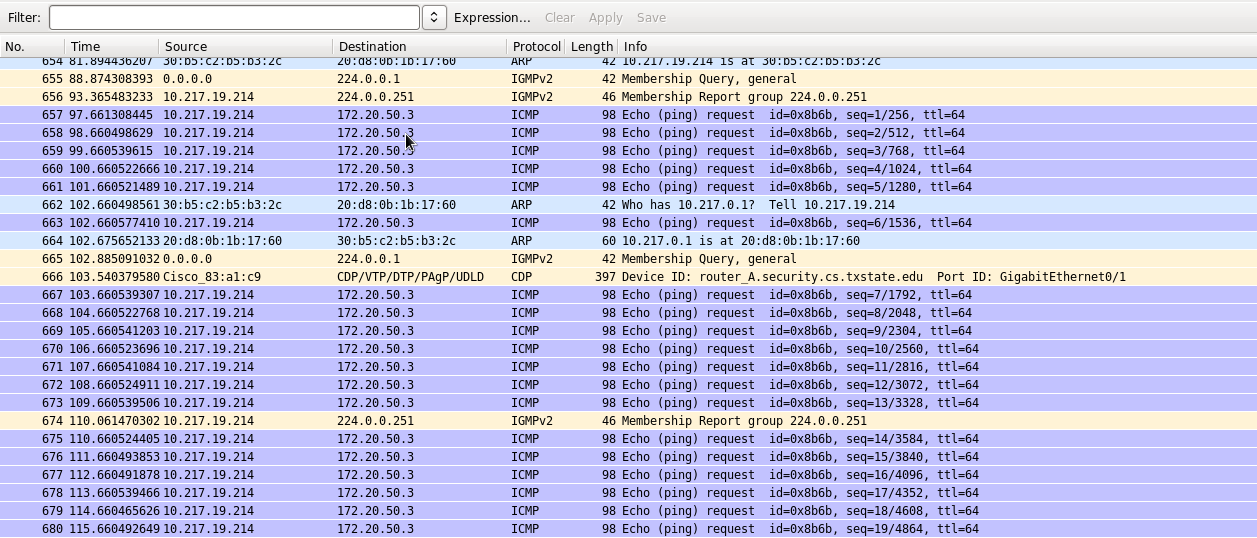


1. Wireshark Results for Ping (Default Firewall)
   1. B.1 Pings B.2

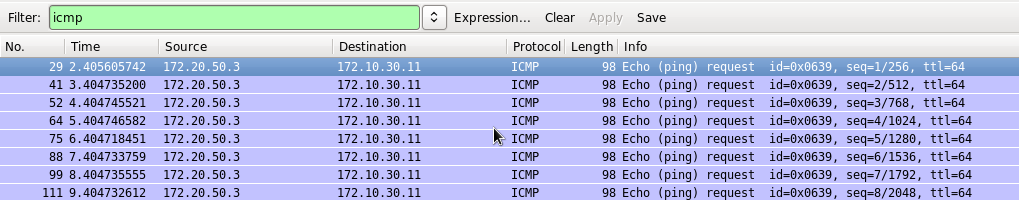
* B.1 could ping B.2



* 1. A Pings B.2
* A could not ping B.2



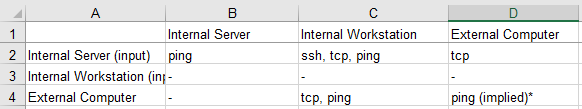
* 1. B.1 and B.2 Ping A
* B.1 and B.2 could not ping A



1. Default Cisco Firewall Policy

The default Cisco firewall policy allowed external computers to access web services of other external computers. It blocked web services to and from internal computers to external computers. It allowed external computers to ping other external computers, but blocked pinging to and from internal and external systems.

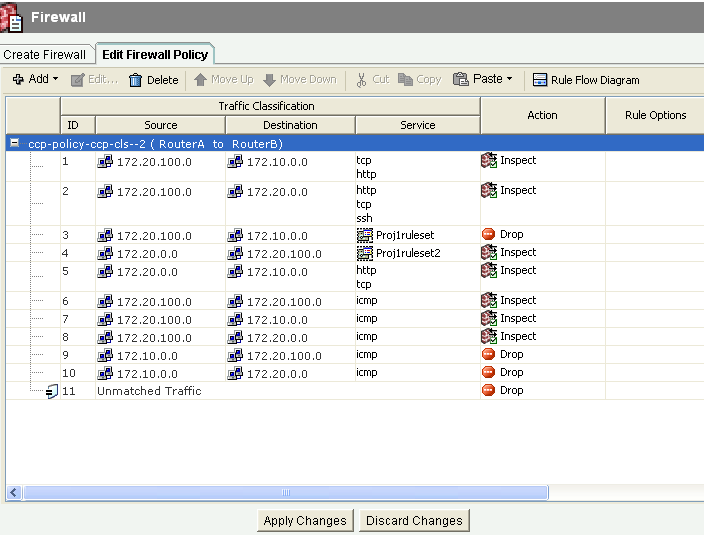
**Section III**

1. ****
2. Cisco Firewall Policy Enforcement

There is one policy that cannot be enforced by the Cisco firewall because of conflicting rules that are enforced higher in the policy and that is policy f: “Internal workstations can access only the web service provided by external computers”. This is unable to be enforced because of policy b and policy c which state that internal workstations are provided web service by the internal servers and the internal servers shall not access any service provided by any external computer. Because of the order of this rule set the internal workstation would be unable to access any service provided by external computers.

The security policy that can only partially be enforced by the Cisco firewall is h: “External computers cannot ping to any internal computers”. Because of rule a: “Internal servers provide only web service to external computers”, external computers that are provided web service by internal servers will have the ability to ping those servers but still be unable to ping internal workstations.

1. Cisco Firewall Configuration



1. Enforcement Using iptables

The Iptables are a command line firewall that uses policy chains to grant or deny traffic. The iptables sequentially compares packets to a set of rules. Once a packet matches a rule an associated action is executed, and the packet is not compared to the remaining rules. The user can create chains as needed. There are three initial default chains which are input, output and forward. The input chain manages all packets that are addressed to the user’s server, the output chain possesses rules for the traffic created by the user’s server and the forward chain is used to handle traffic that is being sent to servers that were not created by the user’s server.

User’s must be aware that the order of the rules associated with each chain matter. This is because a packet must not match with a general rule when there is a more specific rule that follows. This means users should implement the rules with a higher level of specificity at the top of the chain. If a packet falls through the entire chain, it will then reach the default policy. This reasoning determines the rules that will be included in a chain. A chain that has a default policy to accept will possess rules that drops packets and a chain that has a default policy to drop packets will possess rules to specify packets to be accepted. Therefore, iptables rules must be created to regulate the internal traffic between computers with server IPs and computers with workstation IPs.

In conclusion iptables are required to manage internal traffic rules for policies B and E. These two policies allude to the fact that the servers should provide the necessary services of web and SSH to the workstations. With that being stated iptables rules are a requisite to maintain this internal traffic between computers with server IPs and computers with workstation IPs.

1. Iptables Commands

b.) Internal servers provide only SSH and web services to internal workstations.

sudo iptables -A INPUT -p tcp -s 172.20.50.0/24 --dport 22 -m conntrack --ctstate NEW, ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -p tcp -sport 22 -m conntrack -ctstate ESTABLISHED -j ACCEPT

sudo iptables -A INPUT -p tcp -m multiport -dsports 80,443 -m conntrack -ctstate NEW, ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -p tcp -m multiport --dsports 80,443 -m conntrack --ctstate ESTABLISHED -j ACCEPT

e.) Internal workstations can access the services hosted by internal servers.

sudo iptables -A INPUT -p tcp -s 172.20.50.0/24 -j ACCEPT

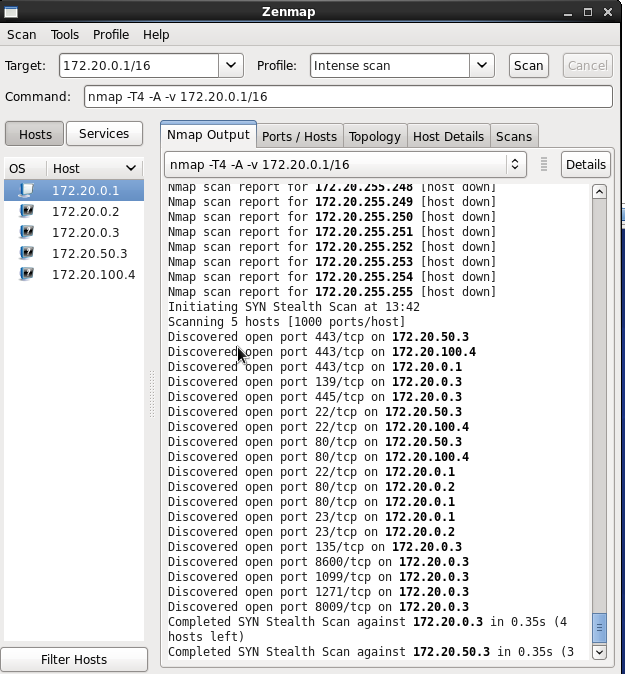
sudo iptables -A OUTPUT -p tcp -d 172.20.0.0/16 -j ACCEPT

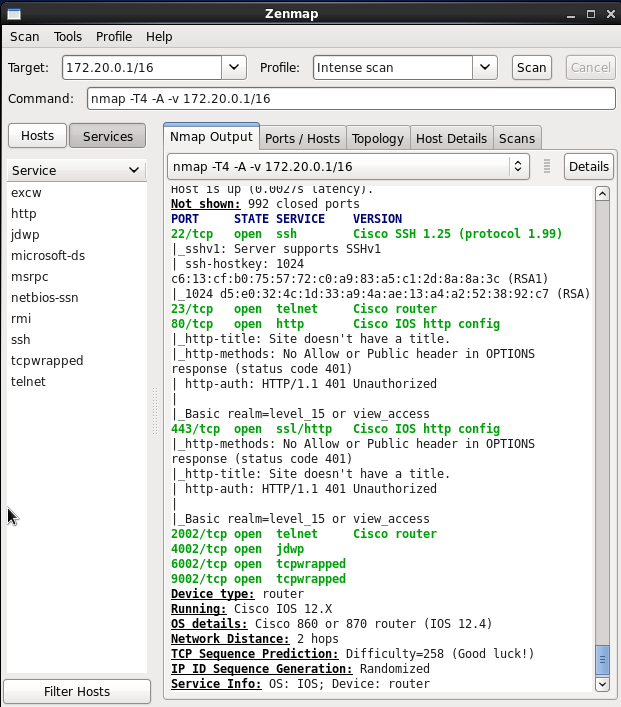
sudo iptables -A INPUT -p udp -s 172.20.0.0/16 -j ACCEPT

sudo iptables -A OUTPUT -p udp -d 172.20.0.0/16 -j ACCEPT

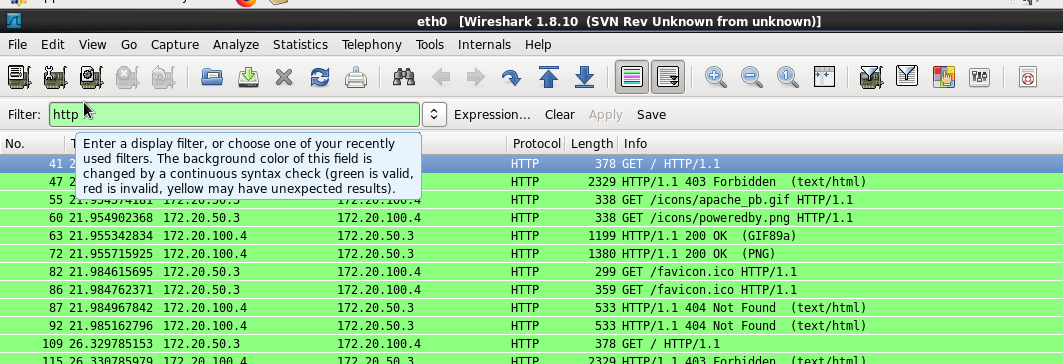
**Section IV**

1. NMap Results With Configured Cisco Firewall
   1. Computers/Hosts

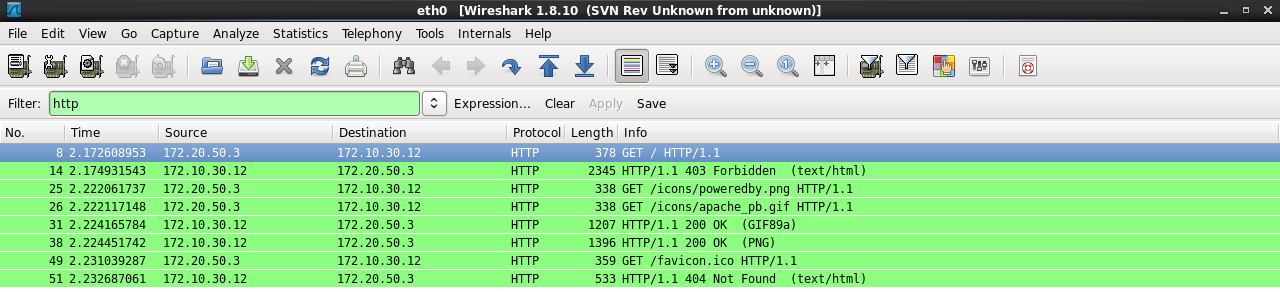


* 1. Service Ports

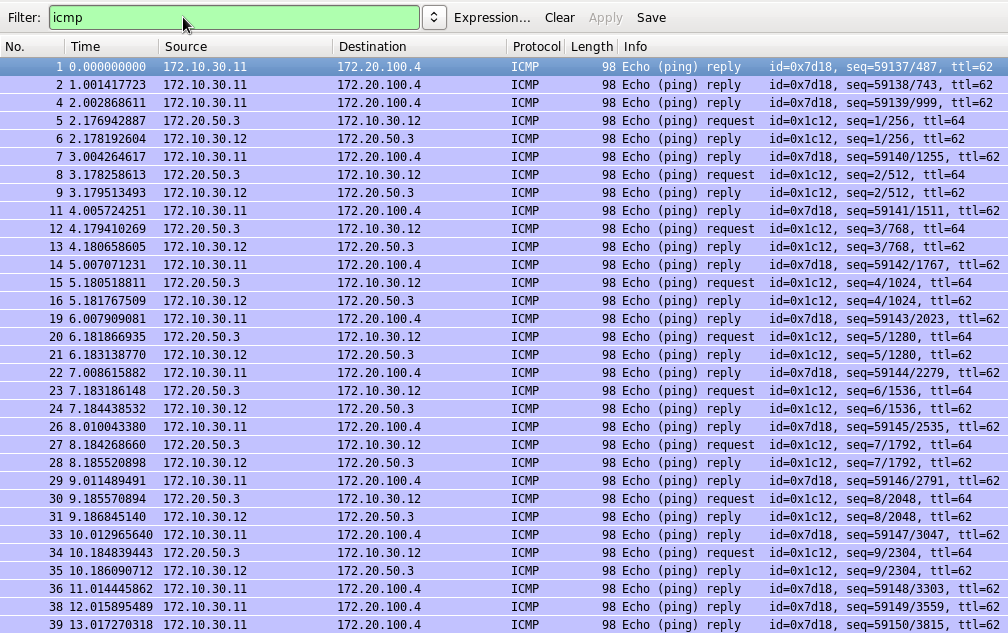
1. Wireshark Results for Web Services With Configured Cisco Firewall
   1. B.1 access web services of B.2 (Allowed)

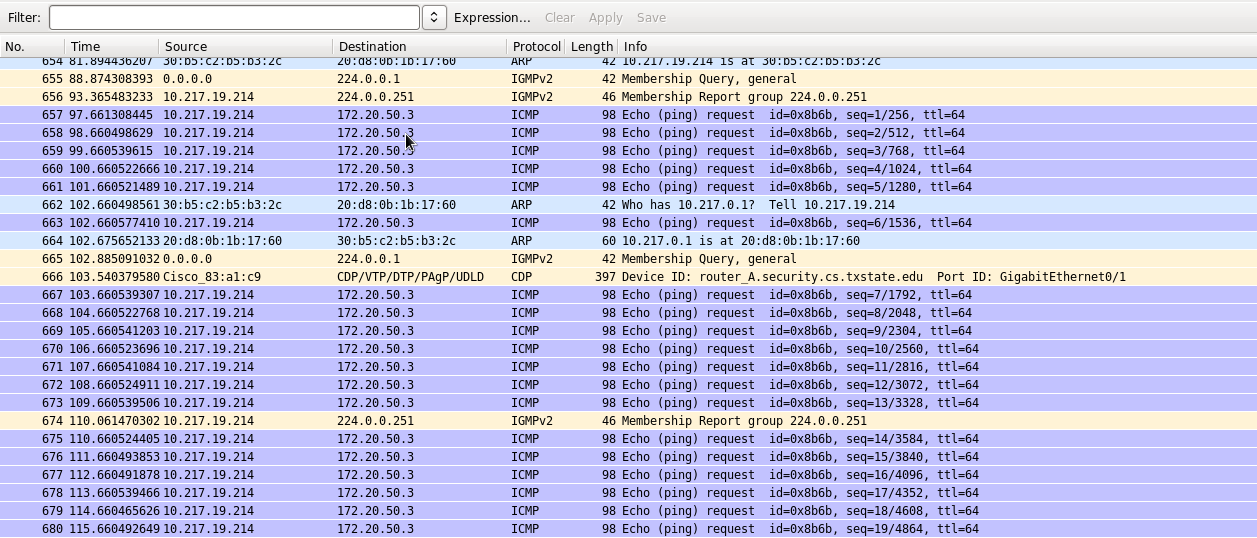


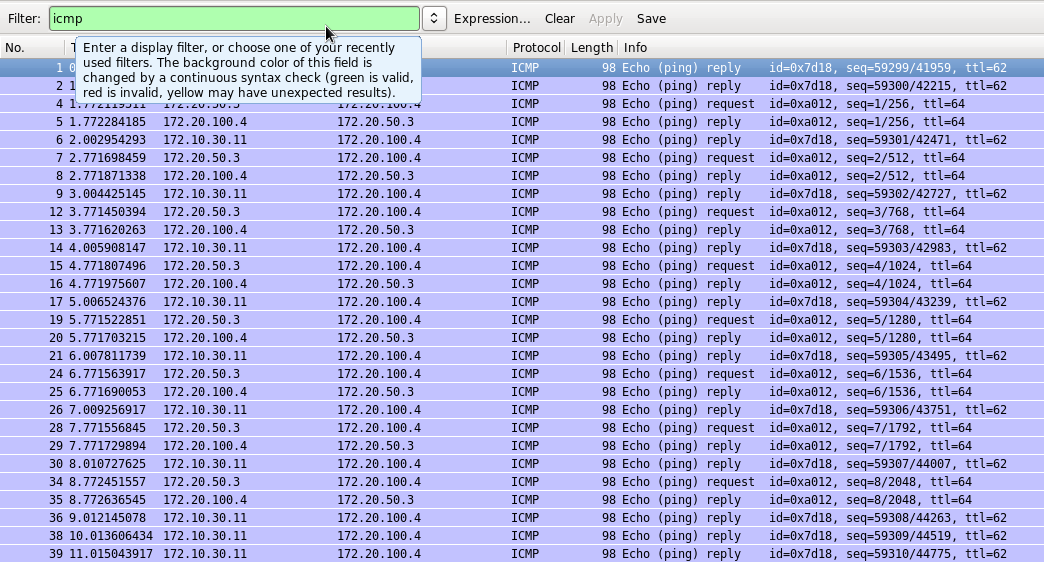
* 1. A access web services of B.1 and B.2 \
* The screenshot for this section was lost.
  1. B.1 and B.2 access web services of A (Allowed)



1. Wireshark Results for Ping With Configured Cisco Firewall
   1. B.1 Pings B.2 (allowed)



* 1. A Pings B.2 (not allowed)
  2. B.1 and B.2 Ping A (allowed)



1. Security Policy Scenario

B.1 is the only computer to store classified information, but can still be accessed because of rules A and B. Rule B states “Internal servers (B.2) provide only SSH and web services to internal workstations (B.1). The problem here is that if a malicious user logs into B.2 then they can transfer files to B.1 using SCP by having access to SSH. Rule A states “Internal servers provide only web service to external computers.” This allows B.1 to release its files over the web which is a security issue. Rule C places some safeguard over this by not letting external computers access B.1 through the web (or any service). In general, if there is a malicious user who has the credentials to an internal server and internal workstation, they will be able to transfer the classified files, as long as those credentials have access to those files.