Checkpoint 4 – **6%**

**Upon submission of your documentation for Checkpoint #4,** We will be testing your ability to manipulate the firewall (iptables.) To accomplish this, you will write three (3) different scripts according to the specifications below. These scripts will change your iptables configuration depending on the services that are to be allowed or denied. We will then test the firewall using the various methods of evaluation listed for each scenario. All traffic must also be blocked or accepted through the use TCP/UDP PROTOCOL port number filtering. **All traffic must be logged by iptables whether it is dropped or accepted.**

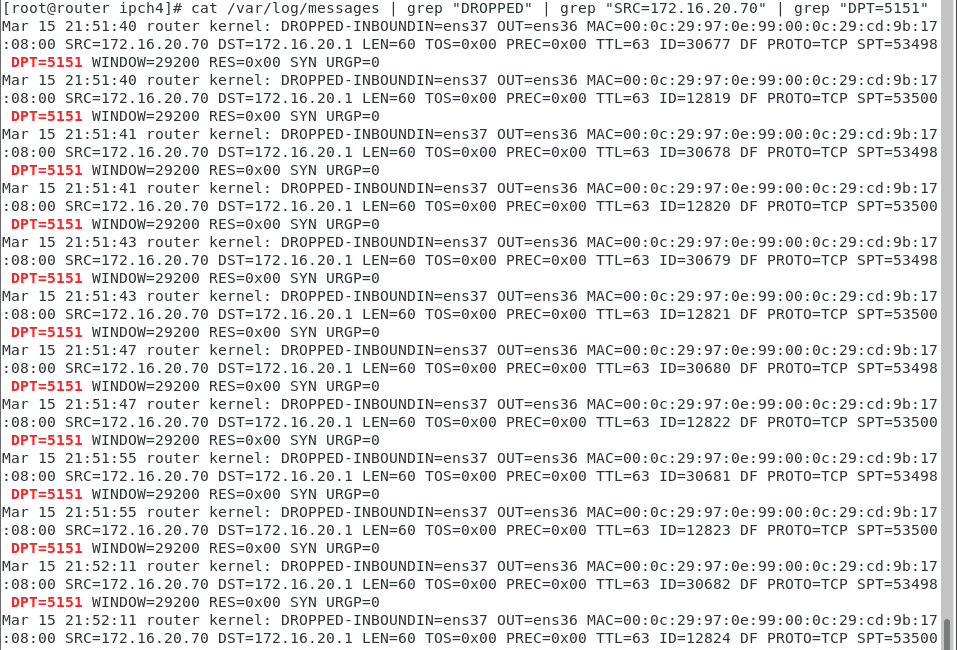
|  |  |  |
| --- | --- | --- |
| Service | Configuration | Method of evaluation |
| Scenario 2 | **All requests to servers will be dropped except for the following:**  DHCP  DNS  SSH to the router  IIS web server  Mysql server | You will demonstrate access to relevant services upon my request and denials to unauthorized services upon my request. You will run an NMAP scan of your **Linux Router, Windows server and Linux Server** and include the report in your documentation. |
| Scenario 3 | **All requests to servers will be dropped except for the following:**  DHCP  DNS  SSH to the router | You will demonstrate access to relevant services upon my request and denials to unauthorized services upon my request. You will run an NMAP scan of your **Linux Router, Windows server and Linux Server** and include the report in your documentation. |
| Scenario 4 | **All responses from servers will be dropped except for the following:**  DHCP  DNS  SCP  Unencrypted FTP | You will log in to each FTP service from the client and download a file. You will run an NMAP scan of your **Linux Router, Windows server and Linux Server** and include the report in your documentation. |
| LOGGING | Iptables must log **ALL** traffic. | You will demonstrate that iptables has logged traffic creating a file that contains log information for specific traffic at specific dates and times. See the requirements below in the required documentation example. |

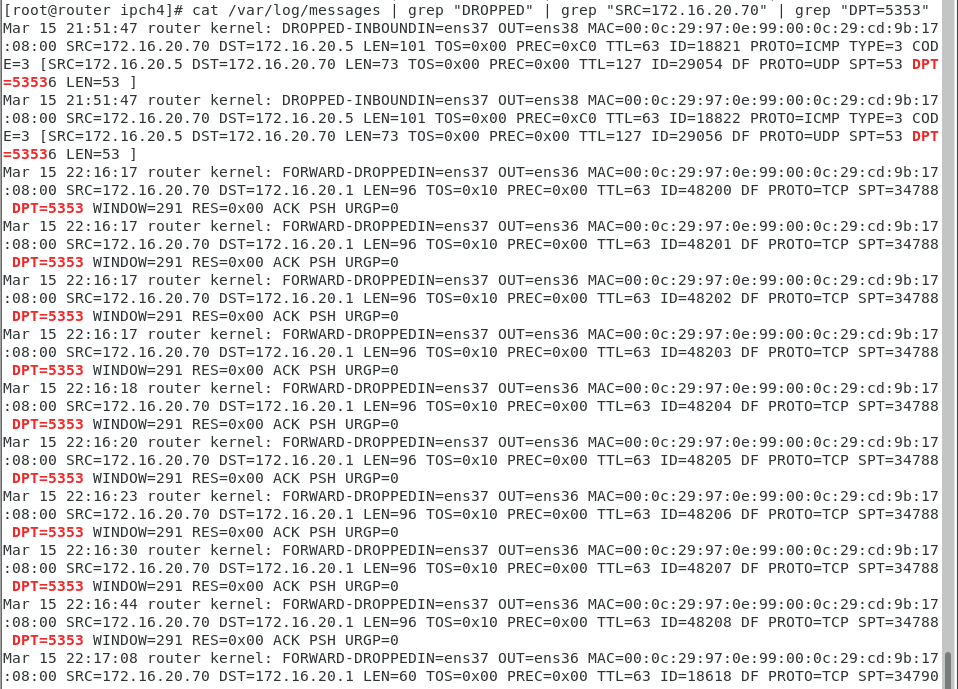
Required documentation:

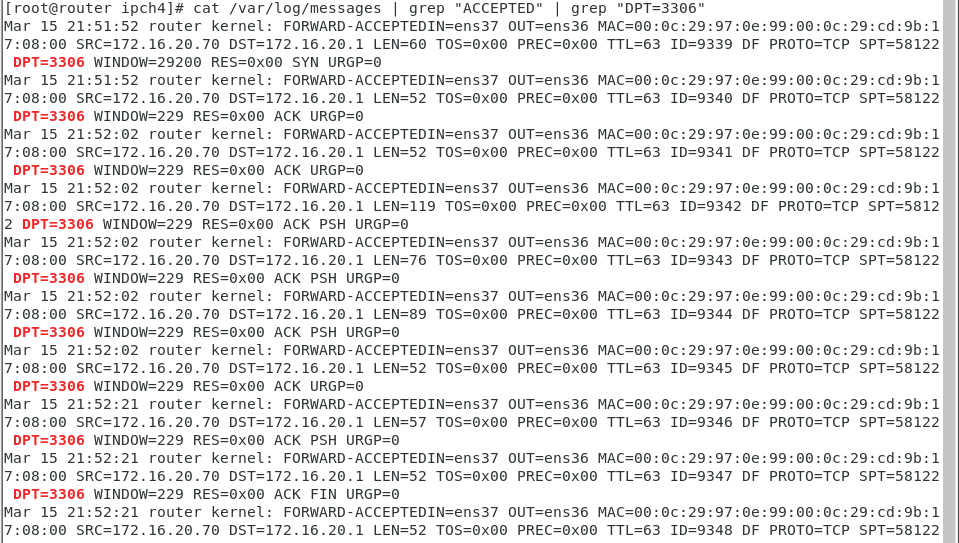
All iptables scenario scripts

Filtered iptables log for all traffic **ON THE DAY OF THE DEMONSTRATION.** Please include ONE PACKET for each of the following:

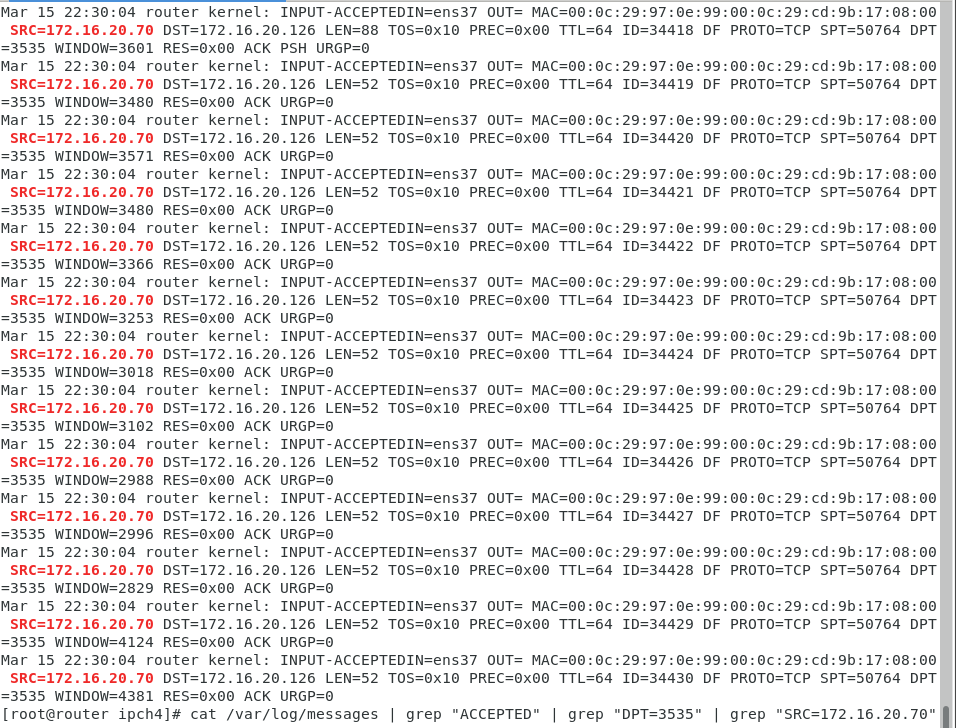
* A DROPPED APACHE request from you Client



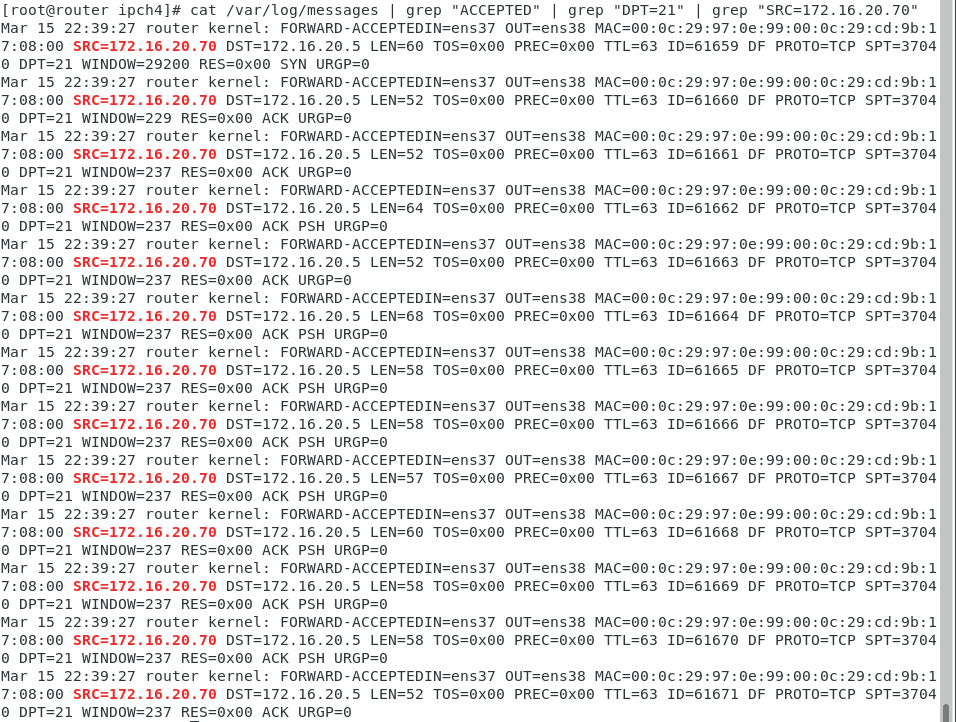
* A DROPPED APACHE response from your Linux Server
* A DROPPED SSH request to your LINUX Server
* 
* A DROPPED IMAP response from your Windows Server
* AN ACCEPTED MYSQL request from your Client



* AN ACCEPTED SSH request to your router



* AN ACCEPTED FTP response from your Windows Server (Port 20)



The results of all NMAP scans