Firewall Logs

In this activity I will be analyzing a Firewall wall log to answer the following questions.

1. How many different ports did the attacker attempt to access?

The attacker tried to access twelve ports: 21, 22, 23, 53, 80, 139, 443, 445, 1453, 1521, 3306, 3389

1. What kind of attack/activity could have been made according to the logs above?

When looking at the log, this was likely a port-scan activity from the constantly changing destination port.

1. How does Firewall determine whether to forward an incoming packet to the destination or not?

The Firewall determines whether to forward an incoming packet to the destination port according to the rule policy.

1. How many open ports did the attacker detect?

The attack detected three open ports shown by “action=allow”.

1. Will the attacker get a response from the Firewall stating that its access request was blocked?

Yes, the attacker will get a response as the “action=deny” which blocks the packet transmission while returning information to the IP informing that it was blocked. If instead “action=drop” the attacker would receive no response after the packet was dropped.

Web logs

1. Are there any SQL injection attacks with a status code of 200? (True or False)

By using the command “cat http.log | egrep -i 'select|union|insert|concat' |grep '200' |grep 'OK' | wc -1” I can find the amount of lines in the log file that contain common SQL commands and were successful. To break down the command:  
Cat http.log: reads contents of http.log

“|”: Pipe allows you to send the output of the previous command as the input to the next command.

Egrep -i ‘select|union|insert|concat|’: extended grep that searches for lines containing case sensitive common variables in SQL quires

Grep 200: filters output to include lines only containing the HTTP status code for 200 or successful requests

grep ‘OK’: include only lines containing ok

Wc -l: word count utility that counts the number of lines.

After running this command the result found 298 matching lines of queries.

If you wanted more information on the logs you could replace ‘wc -l’ with ‘more’ to show the collected information page by page.

1. Identify the highest requesting IP address.

Using the command ‘cat http.log | awk '{print $3}' |sort -n |uniq -c | sort -n’ found that the highest requesting IP address was 192.168.203.63 making 1289498.

1. How many web requests are made with "DELETE" method in total?

Using the command ‘cat http.log | awk '{print $8}' | grep -w DELETE | wc -l’ found that there are 223 web requests made with the delete command in total.

1. Are there web logs with “Nmap Scripting Engine” in the user-agent information among the web requests made? (True or False)

Using the command ‘cat http.log | egrep "Nmap Scripting Engine" | wc -l’ found there were several logs with “Nmap Scripting Engine” in the user-agent information among the web requests made.