1 EASY)

We have an urgent issue with the firewall, none of the staff can access the internet at all. Before you worry about safety I need you to get us back online immediately.\n\n<font size=\"*13\*">**<B> It seems like the policy for the firewalls INPUT and OUTPUT tables have been set to DROP so all incoming and outgoing packets are dropped by default.</B>** </font size=\"*13\*">\n\n You need to either change the default policy for these chains or add sufficient rules to allow internet access, \n\n To edit the firewall you will need superuser privilege, which is gained by using “sudo” before the desired command.\n\n To edit the firewall use the “iptables” flag followed by a series of commands and corresponding parameters. For example to change a chains default policy use the “-P” or “--policy” command followed by the chain name and desired default policy, valid policies are “DROP” , “ACCEPT” and “REJECT” \n\n<font size=\"*13\*">**<B>** sudo iptables -P INPUT ACCEPT**</B>** </font size=\"*13\*">\n\n To learn more about more commands or command structure you can use the “-h” or “--help” command i.e:\n\n<font size=\"*13\*">**<B>** sudo iptables --help**</B>** </font size=\"*13\*">\n\n Once you are happy with the changes you have made to the firewall, click the “Submit” button to see if you have completed the task.

1 MED)

The firewall seems to be blocking the internet access for the office, we need this fixed right away\n\n <font size=\"*13\*">**<B>**I suggest looking at the OUTPUT and INPUT table's default policy **</B>**</font size=\"*13\*"> or adding some rules to the chains to allow traffic in and out, don’t worry about security at the moment \n\n Try using <font size=\"*13\*">**<B>**-L **</B>**</font size=\"*13\*"> to list current rules and table policy, <font size=\"*13\*">**<B>-A</B>**</font size=\"*13\*"> to append a rule to a table and <font size=\"*13\*">**<B>-P</B>**</font size=\"*13\*"> to change a tables policy if needed, Don't forget to try <font size=\"*13\*">**<B>--help</B>**</font size=\"*13\*"> for some information on how to use the iptable commands\n\n <font size=\"*13\*">**<B>** To edit the firewall you will need superuser privilege, remember to type sudo before the 'iptables' command.\**</B>**</font size=\"*13\*">\n\n Once you are happy with the changes you have made to the firewall, click the “Submit” button to see if you have completed the task.

2 EASY)

We are vulnerable to all malicious hackers out there, we need some protection.\n\n I want you to update the firewall such that only incoming TCP packets on ports 80 and 443 are accepted and all others are dropped\n\n To add a rule to a chain use the “-A” or “--append” command followed by the chain name on which the rule should be added, and also followed by a range of options which define the rule. For example the option “-j” or “--jump” tells the rule what to do with a packet that is a match with the main section of the rule, by default iptables allows four targets: “ACCEPT”, “REJECT”, “DROP” and “LOG”. Options for the rule include “-p” or “--proto” which specifies the protocol and “--dport” specifies the destination port, these options are used to match corresponding packets i.e:\n\n <font size=\"*13\*">**<B>** sudo iptables -A INPUT -j ACCEPT **--dport 80 -p tcp</B>**</font size=\"*13\*">\n\n Remember that rules are applied by first match, try to think about your INPUT tables chosen default policy and if you need to add an extra rule at the end to specify what to do with unmatched packets.

2 MEDIUM)

We are vulnerable to all malicious hackers out there, we need some protection.\n\n I want you to update the firewall such that only incoming TCP packets on ports 80 and 443 are accepted and all others are dropped\n\n <font size=\"*13\*">**<B>**Try to use the insert “-I” or append “-A” commands along with “--dport” destination port, “-p” protocol and “-j” jump options to create your rules.**</B>**</font size=\"*13\*">\n\n Remember that rules are applied by first match, try to think about your INPUT tables chosen default policy and if you need to add an extra rule at the end to specify what to do with unmatched packets

3 EZ)

I’m still not sold you’re the person for the job, I’ve tinkered with the firewall a little bit, let’s see if you can get things working correctly again!\n\n Use “-D” or “—delete” to remove a rule: \n\n <font size=\"*13\*">**<B>sudo iptables -D INPUT 3</B>**</font size=\"*13\*">

3 MED)

I’m still not sold you’re the person for the job, I’ve tinkered with the firewall a little bit, let’s see if you can get things working correctly again!\n\n Use “-D” or “—delete” to remove a rule.

3 HARD)

I’m still not sold you’re the person for the job, I’ve tinkered with the firewall a little bit, let’s see if you can get things working correctly again!

4 EASY)

If you’re going to work here I value efficiency, I want you to again fix the firewall that I have broken, but this time try to do it with as few commands as you can manage. Use “-F” or “--flush” to delete all rules or all rules in a chain:\n\n<font size=\"*13\*">**<B>sudo iptables -F OUTPUT</B>**</font size=\"*13\*">

4 MEDIUM)

If you’re going to work here I value efficiency, I want you to again fix the firewall that I have broken, but this time try to do it with as few commands as you can manage. Use “-F” or “--flush” to delete all rules or all rules in a chain.

4 HARD)

If you’re going to work here I value efficiency, I want you to again fix the firewall that I have broken, but this time try to do it with as few commands as you can manage.

5 EZ)

One of the staffers needs to use SMP and as such inserted a rule into the INPUT chain.\n\n It seems like they used the incorrect port number, SMP by default runs on port <font size=\"*13\*">**<B>**445**</B>**</font size=\"*13\*"> use the “-R” or “--replace” command to change the incorrect rule to the correct rule with the appropriate port i.e:\n\n<font size=\"*13\*">**<B>sudo iptables -R 5 --dport 123 -j ACCEPT -p tcp</B>**</font size=\"*13\*">

5 MEDIUM)

One of the staffers needs to use SMP and as such inserted a rule into the INPUT chain.\n\n It seems like they used the incorrect port number, SMP by default runs on port <font size=\"*13\*">**<B>**445**</B>**</font size=\"*13\*"> use the “-R” or “--replace” command to change the incorrect rule to the correct rule with the appropriate port.

5 HARD)

One of the staffers needs to use SMP and as such inserted a rule into the INPUT chain.\n\n It seems like they used the incorrect port number, SMP by default runs on port <font size=\"*13\*">**<B>**445**</B>**</font size=\"*13\*"> use the replace command to change the incorrect rule to the correct rule with the appropriate port.

6 EZ)

Blocking outbound traffic is of benefit in limiting what an attacker can do once they've compromised a system on the network.\n\n As such I’d like to move forward with a default policy change of drop on our OUTPUT chain.\n\n I’ve added the policy change already I need you to add the output rules of the corresponding input rules that you have previously implemented.\n\n Remember that for outgoing rules we can use “--sport” to specify the source port:\n\n <font size=\"*13\*">**<B>sudo iptables -A OUTPUT –j ACCEPT –p tcp –sport 80</B>**</font size=\"*13\*">

6 MED)

Blocking outbound traffic is of benefit in limiting what an attacker can do once they've compromised a system on the network.\n\n As such I’d like to move forward with a default policy change of drop on our OUTPUT chain.\n\n I’ve added the policy change already I need you to add the output rules of the corresponding input rules that you have previously implemented.\n\n Remember that for outgoing rules we can use “--sport” to specify the source port.

6 HARD)

Blocking outbound traffic is of benefit in limiting what an attacker can do once they've compromised a system on the network.\n\n As such I’d like to move forward with a default policy change of drop on our OUTPUT chain.\n\n I’ve added the policy change already I need you to add the output rules of the corresponding input rules that you have previously implemented.

7 EZ)

There has been word of a malicious attacker at the IP of <font size=\"*13\*">**<B>9.9.9.9</B>**</font size=\"*13\*">\n\n Update the firewall to pre-emptively protect us against this by rejecting all packets from that IP. Use “-s” or “--source” as an option to specify the IP address that a rule pertains to.\n\n<font size=\"*13\*">**<B>sudo iptables -A INPUT -s 9.9.9.9</B>**</font size=\"*13\*">

7 MED)

There has been word of a malicious attacker at the IP of <font size=\"*13\*">**<B>9.9.9.9</B>**</font size=\"*13\*">\n\n Update the firewall to pre-emptively protect us against this by rejecting all packets from that IP. Use “-s” or “--source” as an option to specify the IP address that a rule pertains to.

7 HARD)

There has been word of a malicious attacker at the IP of <font size=\"*13\*">**<B>9.9.9.9</B>**</font size=\"*13\*">\n\n Update the firewall to pre-emptively protect us against this by rejecting all packets from that IP.

8 MED)

You better have enjoyed your day off because your absence and shoddy workmanship has caused big problems for me!\n\n One of our engineers needed to use SSH from home but has told me your firewall is beyond repair! \n\n He attempted to fix your work and add a rule to allow his remote login but apparently you have really done a number on this thing.\n\n Lucky for your employment prospects the internet still seems to be working, but if you can’t get Mikes SSH working and clean up the mess he made then sayonara!! \n\n Like I said to Mike, I don’t want every Tom Dick and Harry working from home so make sure only his IP has access: <font size=\"*13\*">**<B>**139.122.5.5**</B>**</font size=\"*13\*">\n\n Use “-D” or “--delete” to delete a firewall rule and “-F” or “--flush” to clear an entire chain to allow incoming SSH connection use the rule specification “--dport” of 22 or “ssh”

8? HARD)

You better have enjoyed your day off because your absence and shoddy workmanship has caused big problems for me!\n\n One of our engineers needed to use SSH from home but has told me your firewall is beyond repair! \n\n He attempted to fix your work and add a rule to allow his remote login but apparently you have really done a number on this thing.\n\n Lucky for your employment prospects the internet still seems to be working, but if you can’t get Mikes SSH working and clean up the mess he made then sayonara!! \n\n Like I said to Mike, I don’t want every Tom Dick and Harry working from home so make sure only his IP has access: <font size=\"*13\*">**<B>**139.122.5.5**</B>**</font size=\"*13\*">

<font size=\"*13\*">**<B></B>**</font size=\"*13\*">