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 EZ)

There is an effective new ransomware going around, for extra security incase any of our computers get infected, i'd like you to drop connetions back to the C&C center so that the RSA encryption keys are not sent and files will not be encrypted.\n\n The current known IP for the C&C center is <font size=\"*13\*">**<B>216.3.3.3</B>**</font size=\"*13\*">.\n\n Remember that the randsomware will be is sending packets from inside the network so you need to drop the connection from the OUTPUT chain. <font size=\"*13\*">**<B>Use “-d” or “--destination” to specify a destination IP address in a rule specification:</B>**</font size=\"*13\*"><font size=\"*13\*">**<B>\n\n sudo iptables -A OUTPUT -j DROP -d 216.3.3.3</B>**</font size=\"*13\*">

8 med)

There is an effective new ransomware going around, for extra security incase any of our computers get infected, i'd like you to drop connetions back to the C&C center so that the RSA encryption keys are not sent and files will not be encrypted.\n\n The current known IP for the C&C center is <font size=\"*13\*">**<B>216.3.3.3</B>**</font size=\"*13\*">.\n\n Remember that the randsomware will be is sending packets from inside the network so you need to drop the connection from the OUTPUT chain. <font size=\"*13\*">**<B>Use “-d” or “--destination” to specify a destination IP address in a rule specification:</B>**</font size=\"*13\*">

**8 hard)**

**There is an effective new ransomware going around, for extra security incase any of our computers get infected, i'd like you to drop connetions back to the C&C center so that the RSA encryption keys are not sent and files will not be encrypted.\n\n The current known IP for the C&C center is <font size=\"*13\*"><B>216.3.3.3</B></font size=\"*13\*">.\n\n**

**9 hard)**

One of our engineers needed to use SSH from home and has attempted to modify the firewall to allow this.\n\n He seems to have caused a bit of a mess, clean up and add the appropriate rules to allow SSH. I dont want everyone working from home so make sure only his home IP of <font size=\"*13\*">**<B>**139.12.12.12**</B>**</font size=\"*13\*"> has access.

9 Med)

One of our engineers needed to use SSH from home and has attempted to modify the firewall to allow this.\n\n He seems to have caused a bit of a mess, clean up and add the appropriate rules to allow SSH. I dont want everyone working from home so make sure only his home IP of <font size=\"*13\*">**<B>**139.12.12.12**</B>**</font size=\"*13\*"> has access.\n\n Use “-D” or “--delete” to delete a firewall rule and to allow incoming SSH connection you need to open port 22.

9 EZ)

**One of our engineers needed to use SSH from home and has attempted to modify the firewall to allow this.\n\n He seems to have caused a bit of a mess, clean up and add the appropriate rules to allow SSH. I dont want everyone working from home so make sure only his home IP of <font size=\"*13\*"><B>139.12.12.12</B></font size=\"*13\*"> has access.\n\n Use “-D” or “--delete” to delete a firewall rule and to allow incoming SSH connection you need to open port 22.\n\n Use “--dport” and “--sport” to specify the port specification for the input and output rules remembering to also specify the TCP protocol with “-p”:\n\n sudo iptables -A INPUT -p x --dport x -s x.x.x.x -j x\n\n sudo iptables -A OUTPUT -p x --sport x -s x.x.x.x -j x**

**10 EZ)**

**I've noticed we dont allow loopback interface connections in our firewall. The loopback interface is used for network connections to itself for example: ping localhost.\n\n Use interface specification options “-i” and -o” on the input and output chains to allow connections on the interface “lo”:\n\n<font size=\"*13\*"><B>sudo iptables -A INPUT -i lo -j ACCEPT</B></font size=\"*13\*">**

**10 MED)**

**I've noticed we dont allow loopback interface connections in our firewall.\n\n Use interface specification options “-i” and -o” on the input and output chains to allow connections on the interface “lo”.**

**10 HARD)**

**I've noticed we dont allow loopback interface connections in our firewall.\n\n Use interface specification options to allow connections on the interface “lo”.**

**11 EZ)**

**On the firewall server we now have one ethernet card connected to the external** <font size=\"*13\*">**<B>(eth0)</B>**</font size=\"*13\*">**, and another ethernet card connected to the internal servers** <font size=\"*13\*">**<B>(eth0)</B>**</font size=\"*13\*">**,.\n\n Use the FORWARD chain to allow internal network talk to external network using the interface specification options “-i” and -o”.\n\n** <font size=\"*13\*">**<B> sudo iptables –A FORWARD -i eth1 -o eth0 –j ACCEPT</B>**</font size=\"*13\*">

**12 EZ)**

**The following rules allow outgoing DNS connections.**

iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT

**13 EZ)**

**I've recenetly read an article about stateless vs stateful firewalls and feel we should re-implement our firewall in a stateful way as they can be better at identifying unauthorized and forged communications.\n\n Iptables supports four states for packets: “NEW”,”ESTABLISHED”,”RELATED” and “INVALID”.\n\n As a start I'd like you to allow established and related incoming connections.\n\n**

**<font size=\"*13\*"><B>To specifify state you need to include the conntrack module by using “-m conntrack” which allows you to use the “--ctstate” option:</B></font size=\"*13\*">\n\n <font size=\"*13\*"><B>sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT</B></font size=\"*13\*">**

**13 MED)**

**I've recenetly read an article about stateless vs stateful firewalls and feel we should re-implement our firewall in a stateful way as they can be better at identifying unauthorized and forged communications.\n\n Iptables supports four states for packets: “NEW”,”ESTABLISHED”,”RELATED” and “INVALID”.\n\n As a start I'd like you to allow established and related incoming connections.\n\n**

**<font size=\"*13\*"><B>To specifify state you need to include the conntrack module by using “-m conntrack” which allows you to use the “--ctstate” option where arguments are seperated with a comma i.e: “--ctstate ESTABLISHED,RELATED”</B></font size=\"*13\*">**

**13 HARD)**

**I've recenetly read an article about stateless vs stateful firewalls and feel we should re-implement our firewall in a stateful way as they can be better at identifying unauthorized and forged communications.\n\n Iptables supports four states for packets: “NEW”,”ESTABLISHED”,”RELATED” and “INVALID”.\n\n As a start I'd like you to allow established and related incoming connections.\n\n <font size=\"*13\*"><B>To specifify state you need to include the conntrack module which allows you to use the “--ctstate” option.</B></font size=\"*13\*">**

**14 EZ)**

**Next thing I'd like you to implement for the stateful firewall is to allow established outgoing connections and to drop invalid incoming packets**

**15 EZ)**

**Given the four states for packets: “NEW”,”ESTABLISHED”,”RELATED” and “INVALID” devise a set of rules to allow incoming HTTP (port 80) connections and incoming HTTPS (port 443) connections.**

**16 HARD)**

**As our network becomes more complex it becomes more prudent to manage all the various connections in more than the three default chains.\n\n Create a new chain called “SSH” using the “-N” command and route all incoming traffic on port 22 to this new chain using the new chain name as the target.\n\n Make the new chains default policy REJECT.**

**16 MED)**

**As our network becomes more complex it becomes more prudent to manage all the various connections in more than the three default chains.\n\n Create a new chain called “SSH” using the “-N” command and route all incoming traffic on port 22 to this new chain using the new chain name as the target.\n\n Make the new chains default policy REJECT.**

**16 EZ)**

**As our network becomes more complex it becomes more prudent to manage all the various connections in more than the three default chains.\n\n Create a new chain called “SSH” using the “-N” command and route all incoming traffic on port 22 to this new chain using the new chain name as the target.\n\n Make the new chains default policy REJECT.\n\n** <font size=\"*13\*">**<B>sudo iptables -N SSH</B>**</font size=\"*13\*">

**17 HARD)**

**Further organisation of chains is in order, create a new chain called “ENGINEERS” which routes all at home traffic from our two engineers Mike and Jan whose IP addresses are** <font size=\"*13\*">**<B>19.19.19.19</B>**</font size=\"*13\*"> and <font size=\"*13\*">**<B>20.20.20.20</B>**</font size=\"*13\*"> respectively.\n\n On this new chain they need you to allow them SSH access and SMP access (port 445) but make sure to reject any other types of packets.\n\n Recall the command for specifying source addresses: “-s”.

**Our network may become too complex to manage all the connections in the three default chains “IN**

**18 h)**

**Just took a look at the new engineers chain you added, the name looks a bit long and messy, shorten it to “ENG” please.**

**18 m)**

**Just took a look at the new engineers chain you added, the name looks a bit long and messy, shorten it to “ENG” please using the “-E” command.\n\n** <font size=\"*13\*">**<B>sudo iptables –E ENGINEERS ENG</B>**</font size=\"*13\*">

**18 EZ)**

**Just took a look at the new engineers chain you added, the name looks a bit long and messsy, shorten it to “ENG” please.**

**18 EZ)**

**more chain stuff**

**19 eZ)**

**The following iptables rule will help you prevent the Denial of Service (DoS) attack on your webserver.**

iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

In the above example:

* -m limit: This uses the limit iptables extension
* –limit 25/minute: This limits only maximum of 25 connection per minute. Change this value based on your specific requirement
* –limit-burst 100: This value indicates that the limit/minute will be enforced only after the total number of connection have reached the limit-burst level.

**20 EZ)**

**You might also want to log all the dropped packets. These rules should be at the bottom.**

First, create a new chain called LOGGING.

iptables -N LOGGING

Next, make sure all the remaining incoming connections jump to the LOGGING chain as shown below.

iptables -A INPUT -j LOGGING

Next, log these packets by specifying a custom “log-prefix”.

iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-level 7

Finally, drop these packets.

iptables -A LOGGING -j DROP

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