Firewall2

Ðàçäåë : Àíàëèòèêà.Îáçîð.

Îïóáëèêîâàíî Son1k [25/11/2010]

Firewall2

û ñ îáùèì ñìûñëîì ”SuSEfirewall – ïëîõî, iptables – õîðîøî”, ðåøèë òàêè ðàçðàáîòàòü ñèì ïîñîáèå, îñíîâàííîì íà ÷òåíèè äîêóìåíòàöèè è ëè÷íîì îïûòå íàñòðîéêè ðåàëüíîãî ÌÑÝ(ìåæñåòåâîãî ýêðàíà)

Ñðàçó îãîâîðþñü. YaST èñïîëüçîâàëñÿ èñêëþ÷èòåëüíî äëÿ íà÷àëüíîé íàñòðîéêè â ñòèëå ”ëèøü áû ðàáîòàëî”. Òîáèøü, ïðîïèñàë âíåøíèé è âíóòðåííèé èíòåðôåéñû, âêëþ÷èë ìàñêàðàäèíã è ïðîïèñàë ìèíèìàëüíûå ôèëüòðû (ncp, ssh, http, https, etc)

Äàëåå îòêðûë ðåäàêòîðîì /etc/sysconfig/SuSEfirewall2 è ïåðâûì äåëîì ïî÷èñòèë îò êîìåíòîâ, ìåøàþò, íó ïðîñòî æóòü êàê.

Âîò, êñòàòè, ÷òî òàêè îñòàâèë, - ïîäñêàçêó ãäå èñêàòü ïîìîùè â ñëó÷àå ×ÀÂÎ.
If you have got any problems configuring this file, take a look at
/usr/share/doc/packages/SuSEfirewall2/EXAMPLES for an example.

Åñëè ýòó îïöèþ âêëþ÷èòü, òî ñêðèïòîì ïðèíèìàþòñÿ âî âíèìàíèå òîëüêî íàñòðîéêè âíåøíèõ èíòåðôåéñîâ, äëÿ âñåõ âíóòðåííèõ îòêðûâàåòñÿ ïîëíûé äîñòóï. Ò.ê. ìíå íàäî áûëî çàêðûòü ïðÿìîé äîñòóï êëèåíòîâ íàðóæó, òî âíóòðåííèå ñåòè ÿ òîæ ïîçàêðûâàë
FW_QUICKMODE="no"

Íó òóò ñîáñòâåííî, ïðîïèñàíû 3 çîíû, êàê âàðèàíò âìåñòî ÌÀÑ ïîæíî ïîäñòàâèòü èìåíà èíòåðôåéñîâ, òèïà eth0, ppp0 è ò.ä.
FW_DEV_EXT="eth-id-00:a0:24:a6:c9:ff"
FW_DEV_INT="eth-id-00:50:04:52:95:e1"
FW_DEV_DMZ=""

Íó ýòî ìíå YaST ñàì íàêîëáàñëè íà ìîå ïðåäëîæåíèå âêëþòèü ìàðøðóòèçàöèþ è ìàñêàðàäèíã íà âíåøíåé ñåòêå, ïðèêîëüêî, ïîëó÷àòñÿ ÷òî ìîæíî îòìàñêàðàäèòü Èíòåðíåò â ñâîþ ñåòóþ ñåòêó.
FW_ROUTE="yes"
FW_MASQUERADE="yes"
FW_MASQ_DEV="$FW_DEV_EXT"

Òóòî÷êè îïèñûâàåì, à êîãî ñîáñòíî ìàñêàäèì. Çäåñü íà÷èíàòñÿ ïðâàÿ ÷àñòü âåñåëüÿ, èáî ìàñêàðàäèòü ìîæíî ïðàâèò÷åñêè êàê õîøü.
10.0.0.0/8 – âñÿ ñåòêà 10.0.0.0/255.255.255.0 õîäèò êóäà õî÷åò, áåç, òàê íàçûâàåìûõ ðåñòðèêöèîíâ
10.0.1.0/24,0/0,tcp,80 – ñåòü 10.0.1.0 áóäåò ìàñêàðàäèòüñÿ òîëüêî åñëè êëèåíò ïîéäåò çà âåá-êîíòåíòîì
10.0.1.0/24,0/0,tcp,1024:65535 – òà æå ñåòü ìàñêàðàäèòñÿ åñëè êëèåíò çàïðîñèò ÷òî-òî èç äèàïàçîíà ïîðòîâ 1024:65535

Åñëè íàäî ïðîïèñàòü íåñêîëüêî ïðàâèë ìàñêàðàäèíãà, òî ðàçäåëÿåì ïîèñêîâÿ ñåòåé ïðîáåëàìè. Íåáîëüøàÿ ðåìàðêà. Íå ðàçîáðàëñÿ åùå ïî÷åìó òàê, íî ñèòóàöèÿ â ñëåäóþùåì, åñëè ïðîïèñûâàåì ìàñêàðàäèíã âñåé ñåòè áåç óêàçàíèÿ ïîðòîâ, òî íàðóæó âûïóñêàåò ïî âñåì ïîðòàì. Ïàðàìåòð FW_AUTOPROTECT_SERVICES="yes" íå ðåøàåò ïðîáëåìó. Òàê ÷òî ëó÷øå óêàçûâàòü êàêîé ñåòè íà êàêîé ïîðò ðàçðåøèòü íàòèòüñÿ.
FW_MASQ_NETS="10.0.50.0/24 10.0.51.0/24,0/0,tcp,22"

Íó òóò âñå ïðîçðà÷íî, âêëþ÷àåì çàùèòó îò âíóòðåííåé ñåòè
FW_PROTECT_FROM_INTERNAL="yes"

Äàëåå àâòîìàòè÷åñêè çàêðûâàåì äîñòóï êî âñåì çàïóùåííûì ñëóæáàì, êðîìå îïèñàííûõ îòäåëüíî
FW_AUTOPROTECT_SERVICES="yes"

Âòîðàÿ ÷àñòü èçâåñòíîãî áàëåòà – ðàñïèñûâàíèå ê êàêèì ñåðâèñàì è ïî êàêèì ïðîòîêîëàì ðàçðåøåí äîñòóï ñíàðóæè. Äîïóñêàåòñÿ çàïèñü êàê íîìåðà ïîðòà, òàê è íàçâàíèÿ ñëóæáû (ïîèñàíé â /etc/services). Ìîæíî óêàçàòü è äèàïàçîí ïîðòîâ. Äëÿ ïàðàìåòðà FW_SERVICES_*_IP òàêæå óêàçûâàåòñÿ ëèáî èìÿ ïðîòîêîëà ëèáî åãî íîìåð. Îòäåëüíûå çàïèñè ðàçäåëÿþòñÿ ïðîáåëàìè.
FW_SERVICES_EXT_TCP="524 8008:8030 http https ssh"
FW_SERVICES_EXT_UDP=""
FW_SERVICES_EXT_IP=""
FW_SERVICES_EXT_RPC=""

Àíàëîãè÷íî äëÿ DMZ...
FW_SERVICES_DMZ_TCP=""
FW_SERVICES_DMZ_UDP=""
FW_SERVICES_DMZ_IP=""
FW_SERVICES_DMZ_RPC=""

... è âíóòðåííåé ñåòè. Íà âñÿêèé ñëó÷àé, îáðàùàþ âíèìàíèå, ÷òî DNS, áåãàåò ïî UDP ïðîòîêîëó, TCP èñïîëüçóåòñÿ òîëüêî â ñëó÷àå åñëè îòâåò ñåðâåðà íå óìåùàåòñÿ â îäíîì ïàêåòå.
FW_SERVICES_INT_TCP="25 110 143 8008 8009 8028 8030 8080"
FW_SERVICES_INT_UDP="53"
FW_SERVICES_INT_IP=""
FW_SERVICES_INT_RPC=""

Âñå âûøåñêàçàííîå îòíîñèòñÿ è ê ýòîìó ïàðàìåòðó, íî îí ïðèíàäëåæèò âî âíèìàíèå òîëüêî åñëè âêëþ÷åí ”áûñòðûé ðåæèì” ÌÑÝ
FW_SERVICES_QUICK_TCP=""
FW_SERVICES_QUICK_UDP=""
FW_SERVICES_QUICK_IP=""

Çäåñü óæå ìîæíî áîëåå òîíêî íàñòðîèòü êîìó è ÷òî èìåííî ìîæíî. Íàïðèìåð, õîñòó 10.0.0.2 ðàçðåøåíî èñïîëüçîâàòü ssh, à âñåé ñåòè – ïðîêñè-ñåðâèñ
FW_TRUSTED_NETS="10.0.0.2,tcp,22 10.0.0.0/24,tcp,3128"

Çàïðåùàåì äîñòóï ê ïîðòàì ñåðâåðà íîìåðîì âûøå ÷åì 1023. Íå ñîâñåì ïîíÿë âàðèàíò DNS, âðîäå êàê ðàçðåøàåò äîñòóï òîëüêî ïîðääëåííûì ñåðâåðàì èìåí.
FW_ALLOW_INCOMING_HIGHPORTS_TCP="no"
FW_ALLOW_INCOMING_HIGHPORTS_UDP="DNS"

Äàííûé ïàðàìåòð çàñòàâëÿåò ÌÑÝ äåòåêòèòü ðàáîòàþùèå ñåðâèñû
FW_SERVICE_AUTODETECT="yes"

Ñîçäàòåëè ïðîãðàììû ðåêîìåíäóþò ïîñòàâèòü yes íàïðîòèâ íóæíûõ ñåðâèñîâ, ÷òîáû îíè ðàáîòàëè. Íå çíàþ, íå çíàþ... ïðîêñþ ÿ ïðîïèñàë â âèäå îòêðûòîãî ïîðòà 8080 íà âíóòðåííåì èíòåðôåéñå è âñå ðàáîòàåò.
Çàïðåùàåì äîñòóï ê DNS
FW_SERVICE_DNS="no"
Çàïðåùàåì ðàáîòó êëèåíòà DHCP (òîáèøü ýòî ñåðâåð óæå â æèçíè íå ïîëó÷èò àâòîìàòè÷åñêîãî àäðåñà)
FW_SERVICE_DHCLIENT="no"
Çàïðåùàåì ñåðâåð DHCP
FW_SERVICE_DHCPD="no"
Çàïðåùàåì ïðîêñè
FW_SERVICE_SQUID="no"
Çàïðåùàåì ñàìáó (ñ ïðåâèëèêè óäîâîëüñòâåì! íàòèãà ñàìáà åñëè åñòü ðàáîòàþùèé ncp?
FW_SERVICE_SAMBA="no"

Ïðîáðîñ. Îïàñíàÿ øòóêà. Ðåêîìåíäóåòñÿ èñïîëüçîâàòü ÒÎËÜÊÎ äëÿ ïðîáðîñà ñîåäèíåíèÿ â DMZ. Ñèíòàêñèñ òàêîâ ”èñõîäíàÿ ñåòü(èëè õîñò), õîñò íàçíà÷åíèÿ”. Ïî æåëàíèþ ìîæíî óêàçàòü åùå ïðîòîêîë è íîìåð ïîðòà. Íàïðèìåð, ”0/0,212.188.4.10,tcp,22” ïðîáðîñèò âñå ñîåäèíåíèÿ íà 22 ïîðò âíóòðåííåãî õîñòà. Àäðåñ íàçíà÷åíèÿ ìîæåò áûòü òîëüêî ðåàëüíûì. Òèïè÷íîå ïðèìåíåíèå – îðãàíèçàöèÿ äîñòóïà ê ïî÷òîâîìó ñåðâåðó.
FW_FORWARD=""

Òîæå ñàìîå ÷òî è àáçàöåì âûøå, òîëüêî äëÿ ïðîáðîñà âî âíóòðåííþþ ñåòü. ×òîáû ñåðâåñ áûë äîñòóïåí è èç âíóòðåííåé ñåòè, íåîáõîäèìî ñäåëàòü ôîðâàðäèíã (ïðåäûäóùèé àáçàö) èç âíóòðåííåé çîíû íà DMZ. Îïÿòü æå, êðàéíå íå ðåêîìåíäóåòñÿ þçàòü ýòó êè÷ó. Íî îíà åñòü. Ïðèìåð, âíóòðè åñòü âåá-ñåðâåð, íàì íóæíî ÷òîá äî íåãî äîñòó÷àëèñü ñíàðóæè. Ïèøåì
FW_FORWARD_MASQ="10.0.0.2,tcp,80 10.0.0.2,tcp,443"

Øòóêà ïîëåçíàÿ äëÿ îðãàíèçàöèè ïðîçðà÷íîãî ïðîêñè, êîãäà íàäî ïðîáðîñèòü ïîðò íà íóæíûé ïîðò íàøåãî øëþçà. Ñèíòàêñèñ ñëåäóþùèé ”èñòî÷íèê (ñåòü/õîñò) íàçíà÷åíèå(ñåòü/õîñò), ïðîòîêîë, ïåðåíàïðàâëÿåìûé ïîðò, ïîðò íàçíà÷åíèÿ”. Íàïðèìåð, "10.0.0.0/8,0/0,tcp,80,3128
0/0,172.20.1.1,tcp,80,8080"
FW_REDIRECT=""

Íó íà ýòî ïîæàëóé âñå. Äëÿ íà÷àëüíîé íàñòðîéêè âïîëíå ñîéäåò. À îñòàëüíîå óæå íþàíñû, êîòîðûå æåëàþùèå ìîãóò ñàìè ðàñêîïàòü. Ñòàòåéêà íå ïðåâîñõîäèò íà 100%, â íåé ìîãóò áûòü îøèáêè. Áóäó ðàä, åñëè ïðèñòóñòâóþùèå ÷òî-òî óòî÷íÿò ëèáî èñïðàâÿò.

Çà ñèì ðàñêëàíèâàþñü.
Loky,
Novell Professional Services

Òîïèàÿ íàñòðîéêà SuSEfirewall2
Technorati Tags: openSuSE, SuSEfirewall2, firewall, configuring
Ñêîïèðîâàíî ïîïàäàëñü ëþäè, êîòîðûå íåðàâíîäóøíî îòíîñÿòñÿ ê âàøåìó

êîìïüþòåðó/ñåðâåðó/ñàéòàì - dos'ÿò, ïûòàþòñÿ âçëîìàòü, ñïàìÿò è ò.ä. Òàêèõ ëþäåé íàäî íåñîìíåííî áàíèòü. Áàíèòü â ôàéðâîëå, ÷òî áû íè îäèí ïàêåò íå äîøåë îò çëîâðåäíîãî ïíëüçîâàòåëÿ. Âîò òóò òî è âñòàåò âîïðîñ, î òîì, êàê ýòî äåëàòü. Â ýòîì ïîñòå ðå÷ü ïîéäåò òîëüêî îá 11îì ñåìåéñòâå SuSE (áîëåå ðàííèå âåðñèè ïðîñòî íå ïðîâåðÿë). Âñå çíàþ, íàñêîëüêî óäîáíàÿ øòóêà SuSEfirewall, õî÷åòñÿ ñêàçàòü ñïàñèáî ðàçðàáîò÷èêàì äëñòðèáóòèâà çà ýòîò ïðåêðàñíûé êîìïíåíò ñèñòåìû. Ôàéðâîëë â SuSE ìîæåò óïðàâëÿòüñÿ êàê ñ ïîìùüþ yast, òàê è ïðàâêîé êîíôèãà â /etc/sysconfig/SuSEfirewall2 Â èíòåðíåòå ïîëíî ñòàòåé ñ íàñòðîéêå ñ ïîìùüþ SuSEfirewall NAT'à, ðàçäåëåíèÿ âíåøíåé, âíóòðåííåé è äåìèëèòàðèçîâàííé çîí, ïðîáîñà ïîðòîâ. Ääèíñòâåííà ÷åãî íåò - òàê ýòî âîçìîæíòè óêàçàòü ñïèñîê ip ääðåñîâ, êîòîðûì íåîáõîäèìî çàïðåòèòü äîñòóï ê ñåðâåðó. Ó ìåíÿ ñåðâåð ïîäêëþ÷åí ê 3 ñåòÿì, ñåòè èíòåðíåò, ëîêàëüíîé ñåòè ïðîâàéäåðà, è ñîáñòâåííîé äîìàøíåé ñåòè. Òàê âîò, ðàíüøå ïðèõîäèëîñü äîáàâëÿòü â ðó÷íóþ ip ääðåñ â òàáëèöó INPUT è ñòàâèòü îí äåéñòâèå DROP. Íî ïðîáëåìà ïðîñòî ýòèì íå ðåøàëàñü, SuSEfirewall îáíîâëÿåò ñâîè ïðàâèëà, è ÷åðåç íåñêîëüêî äíåé çàáàíåííûå àäðåñà ïðîñòî ïðîïàäàþò, ïîýòîìó ðàíüøå ÿ ïðîïèñûâàë èõ ãäå íèáóäü â êîíöå /sbin/SuSEfirewall2 , äàáû îíè âñåãäà äîáàâëÿëèñü ïðè ïåðåçàãðóçêå ññîîâíûõ ïðàâèë. Ýòî áûëî æóòêî íå êðàñèâî è íå óäîáíî, âñå âðåìÿ ðóãàëèñü rkhunter è ossec íà èçìåíåíióþ checksumm äëÿ ýòîãî ôàéëà. ß ïåðåðûë âåñü ãóãë â ïîèñêàõ èíôîðìàöèè ïî äàííîìó âîïðîñó (ïðèì. àâò. Ëèáî ÿ ðåàëüíî íå óìåþ èñêàòü, ëèáî â ãóãëå ðåàëüíî íåò íîðìàëüíîé èíôû ïî SuSEfirewall). Äà õî÷åòñÿ ñêàçàòü, ïî ïîâîäó suse-community, îáðàùàòüñÿ òóäà ÿ äàæå íå ïûòàëñÿ, ïîñëå òîãî êàê ÿ ïîðîñëë îáúÿñíèòü ìíå âîëåå äåòàëüíî íàñòðîéêó wi-fi. Íà îôèöèàëüíîì êàíàëå #opensuse ìíå ïðîñòî êèíóëè ïàðó-òðîéêó ññûëîê. Åñòåñòâåííî ÿ èõ óæå íå ðàç ñìîòðåë è ìíå íè ÷åãî íå äàëî. Íà äàëüíåøèå ìîè ïðîñüáû î ïîìîùè ìíå ñêàçàëè, ÷òî-òî îáèäíå(ïðèì. àâò. äàâíî ýòî áûëî - íåìîìíþ :-]) è ñêàçàëè, ÷òî áû ÿ íå çàäåðæèâàë èõ âðåìÿ. Ïîñëå ýòîãî ñëó÷àÿ ÿ áîëüøå íå ðàçó òóäà íå îáðàùàëñÿ, äà è íåçà÷åì áûëî Ïîòîì ÷òî ÿ ñ÷èòàþ, ÷òî ëó÷øàÿ ïîìîùü òîëüêî â googl'å. Âîáùå, ÿ ñ÷èòàþ, ÷òî íàñòîÿùèé ïðîôåññèîíàë èëè òîò êòî õî÷åò ñòàòü èì, äîëæåí ñíà÷àëà èçëàçèòü âñå ïîèñêîâèêè â ïîèñêàõ îòâåòà, à ïîòì áåñïîêîèòü áîëåå îïûòíûõ òîâàðèùåé, ïîòîì ÷òî ó íèõ è ïðîáëåìû ïîêðó÷å è âðåìÿ ïîäîææå íàøåãî ñ âàìè.
Ýòî áûëî íåáîëüøîå ëèðè÷åñêîå îòñòóïëåíèå, íî ÷òî-òî ìû äàëåêî îòâëåêëèñü îò òåìû ýòîãî ïîñòà. Òàê âîò âíèìàòåëüíî ïðîñìàòðèâàÿ /etc/sysconfig/SuSEfirewall2 ÿ îáíàðóæèë ïàðàìåòð íîâ íîìåðîì 25FW_CUSTOMRULES. Çàåñü ìîæíî ïðîïèñàòü ïóòü ê ôàéëó äîïîëíèòåëüíûõ ïðàâèë. Â /etc/sysconfig/scripts/SuSEfirewall2-custom
ëåæèò ïðèìåð òàêîãî ôàéëà, âîáùåì îí ñîäåðæèò ôóíêöèè âûçûâàåìûå ïððåä ðàçëè÷íûìè ñîâûòèÿìè(hook'è) ñàìîãî SuSEfirewall. Âîò èõ ñïèñîê ñ ïîÿñíåíèÿìè(ïðèì. àâò. ñïåöèàëüíî ïåðåâåë îïèñàíèÿ):

- fw_custom_before_antispoofing() - âñå ÷òî îïèñàíî â ýòîé ôóíêöèè áóäåò çàãðóæåíî äî òîãî, êàê áóäóò ïðèìåíåíû ëþáûå ïðàâèëà àíòèñïóôèíãà. Æåëàòåëüíî ïðîïèñûâàòü çäåñü ïðàâèëà äëÿ DROP'à íåíóæíûõ broadcast ïàêåòîâ è ïðîòóñêà íåêîòîðûõ ïàêåòîâ ÷åðåç ìåõàíèçì àíòèñïóôèíãà.
- fw_custom_after_antispoofing() - çàãðóçêà âàøèõ ïðàâèë, îïñëå ïðèìåíåíèÿ ïðàâèë äëÿ àíòèñïóôèíãà è îáðàáîòêè icmp-ïàêåòîâ, íî ïåðåä ïðàâèëàìè äëÿ îáðàáîòêè IP ïàêåòîâ. Çäåñü æåëàòåëüíî ïðîïèñûâàòü ïðàâèëà äëÿ çàïðåòà äîñòóïà îïðåäåëåííûõ ip-ääðåñîâ èëè tcp/udp ïîðòîâ.
- fw_custom_before_port_handling() - çàãðóçêà âàøèõ ïðàâèë, îïñëå ïðèìåíåíèÿ ïðàâèë äëÿ àíòèñïóôèíãà è îáðàáîòêè icmp-ïàêåòîâ, à òàêæå îïñëå òîãî, êàê âåñü òðàôôèê ïåðåïðåäåëåí â ñïåöèàëüíûå öåïî÷êè SuSEfirewall: input_XXX,forward_XXX è ò.ä. ,íî ïåðåä ïðàâèëàìè äëÿ îáðàáîòêè IP ïàêåòîâ. Çäåñü æåëàòåëüíî ïðîïèñûâàòü ïðàâèëà äëÿ çàïðåòà äîñòóïà îïðåäåëåííûõ ip-ääðåñîâ èëè tcp/udp ïîðòîâ.
- fw_custom_before_masq()(îïæåò òàêæå èìåíîâàòüñÿ êàê "after_port_handling()") - ïðàâèëà, îïèñàííûå çäåñü áóäóò çàãðóæàòüñÿ ïîñëå îáðàáîòêè IP ïàêåòîâ è TCP/UDP ïîðòîâ, íî ïåðåä ïðîáðîñîì ïîðòîâ èëè ìàñêàðàäèíãà. Èñïîëüçóéòå ýòîò õóê, åñëè âàì îí äåéñòâèòåëüíî íóæåí è íåîáõîäèì!
- fw_custom_before_denyall()(îïæåò òàêæå èìåíîâàòüñÿ êàê "after_forwardmasq()") - ïðàâèëà, îïèñàííûå çäåñü áóäóò çàãðóæåíû ïîñëå ïðîáðîñà ïîðòîâ è/èëè ìàñêàðàäèíãà. Èñïîëüçóéòå ýòîò õóê, äëÿ îòêëþ÷åíèÿ ëîãîâ íåíóæíûõ ïàêåòîâ.

Òàê âîò, ÿ ôèëüòðóþ è ðåêîìåíäóþ ôèëüòðîâàòü âñå íåíóæíûå àéïè àäðåñà â hook'e fw_custom_before_antispoofing() ÷òî áû èñêëþ÷èòü âîçìîæíîñòü ïîïàäàíèÿ ëþáûõ ïàêåòîâ â ñèñòåìó ñ íåíóæíûõ àéïè àäðåñîâ.
Ïðèìåð:

```
fw_custom_before_antispoofing() {
iptables -A INPUT -j DROP -s 10.49.56.211/32
iptables -A INPUT -j DROP -s 10.49.56.211/32
iptables -A INPUT -j DROP -s 10.49.48.196/32
iptables -A INPUT -j DROP -s 10.49.166.252/32
iptables -A INPUT -j DROP -s 10.49.42.2/32
}
```

Ôèëüòðàöèÿ èäåò ïî ëîêàëüíîé ñåòè êîðáèíû òåëåêîì îò íà÷èíàþùèõ dos'åðîâ. Íàäåþñü âû òåïåðü ñòàëè åùå áîëåå óâåðåíû, íàñêîëüêî ãèáêèé è óäîáíûé èíñòðóìåíò ïîäàðèëè íàì ðàçðàáîò÷èêè openSuSE, çà ÷òî Ñïàñèáî È Îãðîìíå!

Èíòåðíåò-øëþç íà áàçå OpenSUSE 10.2. Íàñòðîéêà SuSEfirewall2
÷àñòü âòîðàÿ

SuSEfirewall2 ? óäîáíàÿ íàäñòðîéêà íàä ip_tables
Ñîâðåìåííûå âåðñèè ÿäðà Linux (2.6.x) ñîäåðæàò ìùíûå ñðåäñòâî êîíòðîëÿ íàä IP-òðàôèêîì ? ip_tables, äëÿ åãî íàñòðîéêè ñëóæèò óòèëèòà iptables. Ýòîò ìåõàíèçì îáåñïå÷èâàåò â ÷èñëå ïðî÷åãî òðàíñëÿöèþ àäðåñîâ (DNAT è SNAT), Forwarding è Masquerading. Íà ñàéòå ðàçðàáîò÷èêîâ ïðåäñòàâëåí ïîëíûé íàáîð äîêóìåíòàöèè, âêëþ÷àÿ ðóêîâîäñòâî íà íåñêîëüêèõ ÿçûêàõ. Åäèíñòâåííûé íåäîñòàòîê ? âûñîêàÿ ñëîæíîñòü îñâîåíèÿ ? ñ òî÷êè çðåíèÿ ìíîãèõ ïîëüçîâàòåëåé ïðåâåøåâàò ëþáûå äîñòîèíñòâà. Ïî ýòîé ïðè÷èíå â äèſòðèáóòèâ OpenSUSE âêëþ÷åí óäîáíîå è ïðîſòå â èſïîëüçîâàíèè ñðåäſòâî ? SuSEfirewall2 (ſîêðàùåíſ ? SFW2), ôàêòè÷åſêè ïðåäſòàâëÿþùåå ſîáîé íàäſòðîéêó íàä iptables. Î ïðàâèëüſîì ïðèìåíåíèè ýòîãî èſſòðóìåíòà è ſîéäåò ðå÷ü äàëåå.
Ïðåæäå âſåãî ſîòðåáóåòſÿ íàſòðîèòü ſåòåâûå èſòåðôåſû, â ſðîſòåéſåſ ſëó÷àå äîſòàòî÷íſ äâóõ ? âſåøſåãî è âſóòðåſſåãî. Äîſóſòèſ, ýòî áóäóò eth1(MAC 00:2e:15:fb:61:10) è eth0 (MAC 00:16:ac:47:8f:ad) ſſſîòâåòſòâåſſſ. Ìſæſſ âſſſſſïſüçſâàòüſÿ ðàçäåſſ Network Devices / Network Card êſſôèãóðàòſðà YaST2 (/sbin/yast2) ëèáſ íàáðàòü â êſſſſſïſë ſëåäóþùóþ ſſſſåäſâàòåëüſſſòü êſìàſä:

```
ifconfig eth0 down
ifconfig eth0 10.10.1.1 netmask 255.255.255.0 up
ifconfig eth1 down
ifconfig eth1 195.14.50.94 netmask 255.255.255.248 up
route add default gw 195.14.50.89
```

Î÷åâèäſſ, ÷òſ ſðèâåäſſſûå äëÿ ſðèſåðà IP-àäðåſà è ſåòåâûå ſàſêè ſëåäóåò çàſåſèòü àêòóàëüſſûſè äëÿ âàøåé ſåòè.
Êſſſôèãóðàöèÿ SFW2 õðàſèòſÿ â ôàéëå /etc/sysconfig/SuSEfirewall2. Äëÿ åãſ ðåäàêòèðſâàſèÿ ſſæſſ èſſſſüçſâàòü, íàſðèſåð, âûçûâàåſûé ſſ êëàâèøå F4 âſòðſåſſûé ðåäàêòſſ ôàéſſâſſãſ ſåſåäæåðà mc. Ïðè ſåðåſſſå òåêſòſâûõ ôàéëſâ ſåæäó ÎÑ ſëåäóåò ſſſſèòü, ÷òſ ſðèſÿòôé â Linux ðàçäåëèòåëü ſòðſê ſſſòſèò èç åäèſſòâåſſſãſ ſèſâſëà CR, òſãää êàê â DOS è Windows èſſſſüçóåòſÿ ſàðà CR/LF.
Áſëåå 90 ſðſöåſòſâ ſſſäåðæèſſãſ ôàéëà ? ſſäðſáſûå òåêſòſâûå êſſſåſòàðèè ſ ſðèſåðàſè âſçſſæſûõ âàðèàſòſâ íàſòðſéêè. Âſ èçáåæàſèå äſſñäſſûõ ſøèáſê óäàëÿòü êſſſåſòàðèè íå ðåêſſåſäóåòſÿ ? ſſſèſſ ſðſ÷åãſ â ſèõ ſſſäåðæèòſÿ èſôſðſàöèÿ ſ ſðèſåſÿåſûõ çſà÷åſèÿõ ſſ óſſë÷àſèþ. Äëÿ áûſòðſſãſ àſàëèçà òåêóùé êſſſôèãóðàöèè ſſæſſ èſſſſëüçſâàòü ſëåäóþùóþ êſſàſäó:

```
gawk '{ if(substr($0, 0, 1)!="#") if(substr($0, length($0)-2)!="=""") print $0 }'
```

/etc/sysconfig/SuSEfirewall2 | grep .
gawk ? ïîäõîäÿùåå ñðåäñòâî äëÿ ïîñòðî÷íîé ôèëüòðàöèè áåç èñïîëüçîâàíèÿ ðåãóëÿðíûõ âûðàæåíèé Â ðåçóëüòàòå åå âûïîëíåíèÿ â êîíñîëü áóäåò âûâåäåíî ñîäåðæèìîå êîíôèãóðàöèîííîãî òàéëà â ëåãêî÷èòàåìîì âèäå ? îêàæóòñÿ èñêëþ÷åíû ñòðîêè, íà÷èíàþùèåñÿ ñî çíàêà ?#? (êîìåíòàðèè) ëèáî çàêàí÷èâàþùèåñÿ íà ?=""? (íå ïîðåääëåííûå ÿâíûì îáðàçîì ïàðàìåòðû). ×òîáû íå íàáëþäàòü äëèííóþ êîìàíäó áîëåå îäíîãî ðàçà, ìîæíî ñîõðàíèòü åå, íàïèñàâ, â òàéëå swf2cfg, ïðåäâàðèâ ñòðîêó ?#!/bin/sh? è óñòàíîâèâ ñîîòâåòñòâóþùèå ïðàâà êîìàíäíé chmod 700 swf2cfg. Òåïåðü äëÿ àíàëèçà íàñòðîåê äîñòàòî÷íî íàáðàòü è êîíñîëè ./swf2cfg, îäíàêî, èñïîëüçóÿ ïîäîáíûéôèëüòð, íå ñëåäóåò çàáûâàòü î ñóùåñòâîâàíèè çíà÷åíèé ïî óìîë÷àíèþ.
Ðàññìîòðèì ïîäðîáíååôîàò è íàçíà÷åíèå îñíîâíûõ ïàðàìåòðîâ /etc/sysconfig/SuSEfirewall2.
Ïåðâûì äåëî ñëåäóåò ïîðåäåëèòü, êàêîé èç ñåòåâûõ èíòåðôåéñîâ ÿâëÿåòñÿ âíåøíèì (ïîäêëþ÷åííûì ê ñåòè èíòåðíåò-ïðîâàéäåðà) è âíóòðåííèì (ïîäêëþ÷åííûì ê ëîêàëüíîé ñåòè). Ïàðàìåòð any îçíà÷àåò "âñå ïðî÷èå, íå óêàçàííûå ÿâíûì îáðàçîì èíòåðôåéñû" ? â íàøåì ñëó÷àå òàêîâûå ñ÷èòàþòñÿ ïî óìîë÷àíèþ âíåøíèìè:
• FW_DEV_EXT="any eth-id-00:2e:15:fb:61:10"
• FW_DEV_INT="eth-id-00:16:ac:47:8f:ad"

Ñëåäóþùèå äâà ïàðàìåòðà óêàçûâàþò íà íåîáõîäèìîñòü ìàðøðóòèçàöèè òðàôèêà ìåæäó âíóòðåííèì è âíåøíèì èíòåðôåéñàìè, ïðè÷åì âñå êîìïüþòåðû ëîêàëüíîé ñåòè áóäóò ñêðûò ("çàìàñêèðîâàíû") ïîä åäèíñòâåííûì âíåøíèì IP àäðåñîì, âçÿòûì èç íàñòðîåê óêàçàííîãî â òðåòüåì ïàðàìåòðå âíåøíåãî èíòåðôåéñà:
• FW_ROUTE="yes"
• FW_MASQUERADE="yes"
• FW_MASQ_DEV="$FW_DEV_EXT"
Äàëåå íàäëåæèò ïðåä÷èëèòü ìàñêèðóåìûå ïîäñåòè, ñ óêàçàíèåì ñåòåâûõ ïðîòîêîëîâ è ïîðòîâ, à òàêæå àäðåñîâ, êóäà ðàçðåøàåòñÿ ïåðåíàïðàâëÿòü òðàôèê. Ïîäñåòè ïåðå÷èñëÿþòñÿ ÷åðåç ïðîáåë, äëÿ áîëüøåé ÷èòàåìîñòè ïðèìåðà îíè ðàçìåùåíû ïî îäíîé íà ñòðîêó ñ ïðèìåíåíèåì ñèìâîëà êîíêàòåíàöèè ? îáðàòíîé êîñîé ÷åðòû (ïîñêîëüêó ôàéë÷åñêè ðå÷ü èäåò îá îäíîé ñòðîêå, êîììåíòàðèè äî çàâåðøàþùèõ êàâû÷åê íåäîïóñòèìû). Èòàê, â íàøåì ñëó÷àå íàõîäÿùåìóñÿ â ëîêàëüíîé ñåòè ñåðâåðó 10.10.1.3 ðàçðåøàåòñÿ ñîäåéíÿòüñÿ ñ ëþáûìè âíåøíèìè ñåòÿìè ïî ïðîòîêîëó tcp/ip, ïðè ýòîì äîïóñòèìû òðè ïîðòà íàçíà÷åíèÿ 25 (smtp), 110 (pop3), 5899 (Radmin). Êðîìå òîãî, ðàçðåøàþòñÿ DNS-çàïðîñû ïî ïðîòîêîëó udp. Èìåþùàÿ àäðåñ 10.10.1.20 ðàáî÷àÿ ñòàíöèÿ ïîëó÷åò âîçìîæíîñòü ñîåäèíÿòüñÿ ñ ïî÷òîâûì ñåðâåðîì ïî àäðåñó 195.151.13.100, èñïîëüçóÿ ñòàíäàðòíûå tcp/ip ïîðòû 25/110:
• FW_MASQ_NETS="
• 10.10.1.3/32,0/0,tcp,25
• 10.10.1.3/32,0/0,tcp,110
• 10.10.1.3/32,0/0,tcp,5899
• 10.10.1.3/32,0/0,udp,53
•
• 10.10.1.20/32,195.151.13.100/32,tcp,25
• 10.10.1.20/32,195.151.13.100/32,tcp,110"

Ñëåäóþùèå äâà ïàðàìåòðà âêëþ÷àþò çàùèòó îò âîçìîæíûõ àòàê íà âíóòðåííèé ñåòåâîé èíòåðôåéñ, íî ðàçðåøàþò äîñòóï èç ëîêàëüíîé ñåòè ê ïîðòàì 22 (ssh) è 3128 (proxy) ðîóòåðà:

• FW_PROTECT_FROM_INT="yes"
• FW_SERVICES_INT_TCP="22 3128"

Äàëåå íåîáõîäèìî óêàçàòü âíåøíèå ïîäñåòè, äëÿ êîòîðûõ ÿâíî çàïðåùåí (REJECT) èëè ðàçðåøåí (ACCEPT) äîñòóï ê ïîðàäåëåííûì ñåðâèñàì, ðàáîòàþùèì íà ðîóòåðå. Ñëåäóåò èìåòü â âèäó, ÷òî ïðè îòñóòñòâèè ÿâíîãî ðàçðåøåíèÿ ïàêåòû íå áóäóò ïðîõîäèòü ? ê íèì áóäåò ïðèìåíåíà ïîëèòèêà DROP, â êà÷åñòâå ðåàêöèè íà âîçìîæíóþ àòàêó áîëåå ïðåäïî÷òèòåëüíàÿ, ÷åì REJECT. Ïåðâûì ïàðàìåòðîì çàïðåùàåòñÿ äîñòóï ñ ëþáûõ âíåøíèõ àäðåñîâ íà ïîðò 113 ïî ïðîòîêîëó tcp/ip, âòîðûì äîïóñêàþòñÿ ñîåäèíåíèÿ ñ âíåøíåãî àäðåñà 80.17.230.11 ïî ïðîòîêîëó tcp/ip íà ïîðò 22 (ssh) ðîóòåðà. Âîçìîæíîñòü óäàëåííîãî ïîäêëþ÷åíèÿ ñîçäàåò ïîòåíöèàëüíóþ óÿçâèìîñòü, êàòåãîðè÷åñêè íå ðåêîìåíäóåòñÿ ðàçðåøàòü ssh-ñåññèè ñ ïðîèçâîëüíûõ àäðåñîâ:

• FW_SERVICES_REJECT_EXT="0/0,tcp,113"
• FW_SERVICES_ACCEPT_EXT="80.17.230.11/32,tcp,22"

Äîñòóïíûå èçâíå ñåðâèñû ? óãðîçà áåçîïàñíîñòè ñåòè
Ñëåäóþùèé ïàðàìåòð ïîðåäëÿåò äîñòóïíîñòü îòäåëüíûõ ëîêàëüíûõ ñåðâèñîâ äëÿ âíåøíèõ ïîäñåòåé. Ðå÷ü èäåò, íàïðèìåð, î ïî÷òîâîì ëèñòå âåá-ñåðâåðå, êîòîðûå íàõîäÿòñÿ â ìàñêèðóåìîì ñåãìåíòå ñåòè è íå èìåþò âíåøíèõ IP àäðåñîâ. Íåîáõîäèìî ïîíèìàòü, ÷òî ñàì ôàêò íàëè÷èÿ äîñòóïíûõ èçâíå ñåðâèñîâ ñîçäàåò ñåðüåçíóþ óãðîçó äëÿ áåçîïàñíîñòè âñåé ëîêàëüíîé ñåòè. Ïîòåíöèàëüíûé çëîóìûøëåííèê ìîæåò âîñïîëüçîâàòüñÿ êàê íåäî÷åòàìè êîíôèãóðàöèè, òàê è îáíàðóæåííé óÿçâèìîñòüþ â èñïîëíÿåìîì êîäå. Â ïðèâåäåííîì ïðèìåðå îôðûò äîñòóí ê ïî÷òîâîìó ñåðâåðó 10.10.1.3 ñ âíåøíèõ àäðåñîâ, îòíîñÿùèõñÿ ê ïîäñåòè MTU-Stream, à ñ âíåøíåãî àäðåñà 80.17.230.11 ? ê ñëóæáå óäàëåííîãî àäìèíèñòðèðîâàíèÿ (Radmin):

• FW_FORWARD_MASQ="
• 83.237.0.0/16,10.10.1.3,tcp,25,25,195.14.50.94
• 83.237.0.0/16,10.10.1.3,tcp,110,110,195.14.50.94
•
• 85.140.0.0/16,10.10.1.3,tcp,25,25,195.14.50.94
• 85.140.0.0/16,10.10.1.3,tcp,110,110,195.14.50.94
•
• 85.141.0.0/16,10.10.1.3,tcp,25,25,195.14.50.94
• 85.141.0.0/16,10.10.1.3,tcp,110,110,195.14.50.94"
•
• 80.17.230.11,10.10.1.3,tcp,4899,4899,195.14.50.94

Î÷åðåäíàÿ ãðóïïà èç ÷åòûðåõ ïàðàìåòðîâ âëèÿåò íà êîëè÷åñòâî æóðíàëèðóåìûõ ñîáûòèé. Ñóôôèêñ CRIT ïðåäïèñûâàåò ñîõðàíÿòü â ëîã-ôàéë èíôîðìàöèþ îá îòáðîøåííûõ (DROP) èëè ïðèíÿòûõ (ACCEPT) ïàêåòàõ òîëüêî ïðè óñëîâèè, ÷òî îíè áûëè ðàññìîòðåíû êàê "êðèò÷íûå" ? ñóùåñòâóþùèå äëÿ áåçîïàñíîñòè. Ê òàêîâûì îòíîñÿòñÿ â ÷àñòíîñòè íåîòðûå òèïû icmp-ïàêåòîâ, çàïðîñû íà rpc-ñîåäèíåíèÿ, ïåðåíàïðàâëåííûå ïàêåòû. Ñóôôèêñ ALL òðåáóåò îñòîðîæíîãî ïðèìåíåíèÿ, ââèäó âåðîÿòíîãî ðàçäóâàíèÿ ëîã-ôàéëà è ïåðåïîëíåíèÿ äèñêîâîãî ðàçäåëà:

• FW_LOG_DROP_CRIT="yes"
• FW_LOG_DROP_ALL="no"
• FW_LOG_ACCEPT_CRIT="yes"
• FW_LOG_ACCEPT_ALL="no"

Çíà÷åíèå ñëåäóþùåãî ïàðàìåòðà íà âðåìÿ îòëàäêè ìîæíî óñòàíîâèòü â ?no?, ïîñêå çàâåðøåíèÿ òåñòîâ æåëàòåëüíî âåðíóòü ê èñõîäíîìó ñîñòîÿíèå:

• FW_KERNEL_SECURITY="yes"

Ðåêîìåíäîâàíîå çíà÷åíèå ?yes? ïîçâîëÿåò ðîóòåðó îòâå÷àòü íà icmp-çàïðîñ ?echo request? (òàê íàçûâàåìûé ping), ÷òî ìîæåò áûòü ïîëåçíî ïðè ïðîâåðêå ðàáîòîñïîñîáíîñòè êàíàëà è äîñòóïíîñòè

ñåðâåðà:
• FW_ALLOW_PING_FW="yes"

Çíà÷åíèå ïî óìîë÷àíèþ ?no? çàïðåùàåò èñõîäÿùèé èç ëîêàëüíîé ñåòè ping:
• FW_ALLOW_PING_EXT="no"

Øèðîêîâåùàòåëüíûå ðàññûëêè ìîãóò áûòü ðàçðåøåíû ("yes"), çàïðåùåíû ("no") èëè ðàçðåøåíû äëÿ îòäåëüíûõ ïîðòîâ ("137").
• FW_ALLOW_FW_BROADCAST_EXT="no"
• FW_ALLOW_FW_BROADCAST_INT="no"

Íàçâàíèå î÷åðåäíîé ïàðû ïàðàìåòðîâ ñïîñîáíî ââåñòè â çàáëóæäåíèå. Â äåéñòâèòåëüíîñòè çíà÷åíèå ?yes? ÷èòàåòñÿ êàê "íå ñîõðàíÿòü â ëîã ñâåäåíèÿ îá îòáðîøåííûõ øèðîêîâåùàòåëüíûõ ïàêåòàõ":
• FW_IGNORE_FW_BROADCAST_EXT="yes"
• FW_IGNORE_FW_BROADCAST_INT="no"

Ñëåäóþùèé ïàðàìåòð äîïóñêàåò èñïîëüçîâàíèå ïîëèòèêè REJECT âìåñòî DROP äëÿ âíóòðåííåãî ñåòåâîãî èíòåðôåéñà, ÷òî ñîêðàùàåò âðåìÿ îæèäàíèÿ çëîíûøëåííèêîì ðåàêöèè íà çàïðåùåííûå äåéñòâèÿ:
• FW_REJECT_INT="yes"
Êîíôèãóðàöèÿ âñòóïàåò â ñèëó ïîñëå çàïóñêà /sbin/SuSEfirewall2 ïðè óñëîâèè îòñóòñòâèÿ ñèíòàêñè÷åñêèõ îøèáîê.
Ïîäðîáíàÿ äîêóìåíòàöèÿ ñ ïðèìåðàìè íàõîäèòñÿ â äèðåêòîðèè /usr/share/doc/packages/SuSEfirewall2/.
Ïîìèìî àêêóðàòíé íàñòðîéêè áðàíäìàóýðà äëÿ îáåñïå÷åíèÿ àäåêâàòíîãî óðîâíÿ ñåòåâîé áåçîïàñíîñòè ñëåäóåò ñîáëþäàòü ðÿä ïðàâèë, â òîì ÷èñëå:
• îòáðàñûâàòü ïðåäïî÷òåíèå íàèáîëåå çàùèùåííûì âåðñèÿì ÏÎ è ïðîòîêîëîâ (ssh, vsftpd è ò.ä.)
• ñëåäèòü çà ñîîáùåíèÿìè î âûÿâëåííûõ óÿçâèìîñòÿõ è ñâîåâðåìåííî óñòàíàâëèâàòü "îáíîâëåíèÿ" è "çàïëàòêè"
• èçáåãàòü èñïîëüçîâàíèÿ ÏÎ, èñòî÷íèê ïðîèñõîæäåíèÿ êîòîðîãî âûçûâàåò ñîìíåíèÿ
• îòêàçàòüñÿ (åñëè ýòî âîçìîæíî) îò èñïîëüçîâàíèÿ ðîóòèíãà â ïîëüçó ïðîêñè-ñåðâåðà