

WHITE PAPER

Mitigating Attacks on a Supercomputer with KRSI

Billy Wilson

! "#\$%#&\$' (##%) *+' , &'%' - . /01) , 2 / . #01'3"#4'56 -7'

! "#\$%&! \$ ' ()% ! *+, %\$ - ./0123/0 *4%

! "#\$%&' () *+, (- *+. % /0(1*+, 23*+. % / 4 1 , "567"(
! 78* . %&' (! "#\$%&' () *+, , -) . (

! 996: #67' (; ; ; = > ? > ? (

! 1 . #&@9#(

A6&/6+(B"/#*C6(D69"&*#,(E/.#&"C6/#@#*%/(FABDEG(:&%8*76.(@(/63(H%&C(%H(
C@/7@#%&,(@996..(9%/#&%+0(.#@&#*/I(*/(#\$6(J\$K(L*/"M(N6&/6+5(E#(@++%3.(. ,. #6C.(
@7C*/*.#&@#%&.(#%(3&*#6(C%7"+@&(:&%I&@C.(\$@#*/069#(6&&%&.(*/#%(" / 3 @ / #67(. ,. #6C.(
% : 6&@#*% / .5(P\$*.(&6.6@&9\$(76: +% , .(ABDE(% / (6*I\$#(9%C: " #6(/%76.(*/(@(\$*I\$Q: 6&H%&C@/96(
9%C: " #* / I(FRSTG(6/8*&% / C6/#(76#6&C*/6(3\$6#\$6&(ABDE9@/(. "996..H"++ , (#\$3 @&#(
@##@9N.(% / (@(. " : 6&9%C: " #6&(3*\$%#"#(76I&@7*/I(: 6&H%&C@/965(U*86(:&%I&@C.(@&6(3&*##6/(#%(
76C% / .#&@#6(ABDEV.(@1*+*# , (#%(#&I6#(" / 3 @ / #67(16\$@8*%&(&6+@#67(#%(H*+6. , . #6C(
: 6&C*..% / .0(:&%96..(6M69"#*% / 0(/ 6#3%&N(686/#.0(@/7(. *I / @+.5(D , . #6C(: 6&H%&C@/96(@/7(
ABDE(H" / 9#*% / @+*# , (@&6(C6@. "&67(" . * / I(8@&%".(16/9\$C@&N.(@/7(@/(@786&. @& , (6C"+@#*% / (
.9&*: #5(P\$6(@786&. @& , (6C"+@#*% / (@9#*8*#*6.(@&6(+%II67(@/7(C*#*I@#67(3*#\$(C*/*C@+(
: 6&H%&C@/96(+% ..0(1"#(86& , (6M#&6C6(+%@7.(H%&C(.#&6..(#6.* / I(#%+% . (9@ / (%86&+%@7(@(&* / I(
1"HH6&(@/7(9@".6(+%I.(#%(7&%: 5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(|>(
|</p></div>

!
"#!\$%&' () * +&, (%!
!</p></div>

D, .#6C.(@7C*/*.#&@#%&.(%H(\$*I\$Q:6&H%&C@/96(9% C:"#*/I(FRSTG(.#6.(H@96(#\$6(
7@"/#*/I(#@.N(%H(.69"&*/I(&6.6@&9\$(7@#@ (3*#%\$"#(.@9&*H*9*/I(:6@N(. , .#6C(:6&H%&C@/965(
P\$6,(H@9*+*#@#6(9"##*/IQ67I6(&6.6@&9\$(#\$@#(9%/#&@9#"@++,(9% C6.(3*#\$(#*I\$#(76@7+*/6.(@/7(
.#&*/I6/#(7@#@(.69"&*#,(&6X"*&6C6/#.5(D@#*.H,*/I(1%#\$(#*C6(@/7(.69"&*#,(9%/.#&@*/#.(*(.@/(
%/I%*/I(9\$@++6/I6(\$#@#(%H#6/(&6X"*&6.//%86+(@: :&%@9\$6.(#%(%+7(:&%1+6C.5(P\$*.(:@:6&(
76.9&*16.(@/7(#6.#.(A6&/6+(B"/#*C6(D69"&*#,(E/.#&"C6/#@#*%/(FABDEG0(@/63(W@/7@#%&,(
!996..(T%/#&%+(FW!TG(6M#6/.%*/(/L*/"M5(E#(@++3.(. , .#6C.(@7C*/*.#&@#%&.(#%(:&%I&@C(
86&,(. :69*H*9(@/7@&I6#67(W!T(:%+*9*6.(\$#@#(:%6/#*@++,(@8%*7(#\$6(:6&H%&C@/96(*C:@9#(%H(
+@&I6(W!T(6M#6/.%*/.5(</p></div>

P\$*.(@"#\$%&(3*+(&6H6&(#%(\$6(#69\$/%+%I,(@.(ABDE(169@" .6(*#*(.@(7*.*#9*86(
@9&%/,C(\$#@#(*#.9&6@#%&(9%/#/"6.(#%(" .6*/(\$*.(:&6.6/#@#*%/.(FD*/I\$0(>?>(Y"+,G5(
R%3686&0(#\$6&6@76&(. \$" "+7(16(@3 @&6(\$#@#(\$*#.(#69\$/%+%I,(\$@.(166/(&6H6&&67(#%(@.(LDW(
)SU(R%%N.(1,(L*/"M(N6&/6+(7686+%:6&.(FT%&16#0(>?;Z[[696C16&\(T%&16#0(>?>?G(@/7(
LDW(S&%16.(*/(" .6&Q. :@96(@: :+*9@#*%/.(F]+. @0(>?>?G5(</p></div>

ABDE*(.@(L*/"M(D69"&*#,(W%7"+6(FLDWG(\$#@#(\$%N.(*/#%(\$6(.@C6(N6&/6+ (.69"&*#,(
686/#.(@.(D^L*/"M(@/7(!: :!&C%&0(1"#(&@#\$6&(\$#@/(:&%8*76@ (C@0%&(W!T(6M#6/.%*/0(*#(+6#.(
@/(@7C*/*.#&@#%&(9% C:*+6(@/7(@##@9\$(.C@++0(C%7"+@&(:&%I&@C.(\$#@#(9%/#&%+(3\$6#\$6&(@/(
@9#%*/(*.(@++%367(%&(76/*67(FD*/I\$0(>?>(W@&9\$G5(!/(@7C*/*.#&@#%&(9@/(@##@9\$(#\$6*&(%3/(
9".#%C(9%76(\$#@#(9%/#&%+.(H*+6(@996..0/6#3%&N(@9#*8*#,0(:&%96..(6M69"*#%/0(@/7(C"9\$(
C%&65(</p></div>

P\$*.(#69\$/%+%I,(9@/(:%#6/#*@++,(16(@7%:#67(@.(@/(LDW(%H(9\$%*96*/(\$*I\$Q
 :6&H%&C@/96(9% C:"#*/I5(P\$6(H@9#(\$#@#(LDW.(@&6(7*.@1+67(@#(RST(.#6.(*(:&68@+6/#(
6/%"I\$(\$#@#(_EDP(*/+ "767*/(\$6*&(>?;`(!9*#%/(S+@/([&@H#(H%&(RST(D69"&*#,0(aT%/.*76&(
3\$,(#%#+.(+N6(D^L*/"M(7%/V#(I6#" .67b(F_@#*%/@+0(>?;`G5((W@/,(. , .#6C.(@7C*/*.#&@#%&.(
7*.@1+6(D^L*/"M(169@" .6(%H(\$6/(6I@#*86(:6&H%&C@/96(*C:@9#(*#(\$@.(%/ (1%#\$(. ,/#\$6#*9(
16/9\$C@&N.(@/7(&6@+Q3%&+7(@: :+*9@#*%/.(FL@&@16+0(>?>?G5(</p></div>

B6.6@&9\$*/I(ABDE*(.@(9%/#/"@#*%/(%H(:&68*%" .(&6.6@&9\$(%/())SU(S&%16.(F - *+.%/0(
>?>(Y"/6G5())SU(S&%16.(/)0)I0)/(+%3Q :&%H*+6(@##@9N.(@I@*/.#(.6&86&.(3*#\$(+*##+6(</p></div>

@ 2021 SANS Institute

Author Retains Full Rights

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(| c(
!
:6&H%&C@/96(*C:@9#\\$3686&0(#\$6(:&%16.(36&6(+*C*#67(*/(#\$6*&(@1*+*#,(#%(2'0'3#0)(#\$6(
@##@9N.5(E/(9%/##@.#0(ABDE9@/((:&%8*76(1%#\$(76#69#*%/(@/7(C*#*I@#*%/5(
E/(#\$*.(6.6@&9\$0(/63(#&@9*/I(.9&*:#.(36&6(3&*##6/(\$@#(" .67(ABDE(#%(76#69#(@/7(
C*#*I@#6(+%3Q:&%H*+6(@##@9N(#69\$/*X"6.5(!/(6/8*&%/C6/#(%H(6*I\$#(9%C:"#6(/%76.(3@.(
9%/H*I"670(1%%#67(H&%C(#\$6(+@#6.#(@8@*+@1+6(.#@1+6(L*/"M(N6&/6+(@.(%H(>;D6:#6C16&(>?>?5(
)6/9\$C@&N*/I(%#%+.(36&6(&"/(%/(#\$6(9%C:"#6(/%76.(#%(C6@."&6(#\$6*&(1@.6+*/6(
:6&H%&C@/965(!(.6&*6.(%H(+%3Q:&%H*+6(@##@9N.(36&6(#\$6/(+@"/9\$670(@+%/I(3*#\$(#\$6(#&@9*/I(
.9&*:#.0(7"&*/I(@(.69%/7(.6#(%H(16/9\$C@&N.5(\$6&H%&C@/96(3@.(9%C:@&67(@/7(\$6(
H"/9#*%/@+*#,(%H(#\$6(.9&*:#.(3@.(@/@+,d675(U*86(@::6/7*96.(\$@86(166/*/+*767(#\$@#(
:&%8*76(@ (ABDE("#%#&*+0(8@&*%".(.%"&96(9%760(@/7(16/9\$C@&N(&6."+#.5(
-#!./+0%(1(23!4/5,/6!
-&*#*/I(ABDE(:&%I&@C.(.*(@/(@78@/967(#%:*95(P(C@N6(#\$6("1069#(C%&6(
@::&%@9\$@1+60(@1&*6H(&68*63(%H(#\$6(#69\$/%+*I*6.(\$@#(ABDE*(.1"*+#"(:%/(.*(:&%8*7675(
!"#\$ %&'\$(
ABDE*(."+#*C@#6+, (C@76(:%..*1+6(1,()6&N6+6,(S@9N6#(U*+6&0(%&()SU5(P\$%"IS(
#&@7*#*%/@+*,(69%I/*d67(@.(@(/6#3%&N(H*+6&(#%#%+0()SU*(./%3(@(. ,. #6CQ3*76(#&@9*/I(
."1.,. #6C(H%&(L*/"M5(
e.*/I()SU0(. ,. #6C.(@7C*/*.#&@#%&.9@/(3&*#6(@/7(@##@9\$(.C@+@(#&@9*/I(:&%I&@C.(#%(
:+@96.(%H(*#6&6.#*/(\$6(%:6&@#*/I(. ,. #6C5(P\$6(:&%I&@C.(9@/(16(@##@9\$67(#%(76H*/67(
#&@96:%*/#.(%&(@&1*#&@&, (H"/9#*%/.0(1%#\$(*/(\$6(N6&/6+(@/7(" .6&Q.:@96(F f&6II0(>?>?G5(- \$6/(
@ (H"/9#*%/*.(6/#6&67(%&(6M*#670(#\$6()SU(:&%I&@C(9@/(8*63(#\$6(7@#@(:@..67(#%(\$6(H"/9#*%/(
@/7(7@#@(&6#"&/67(H&%C(#\$6(H"/9#*%/5(P\$%"IS(" .67(:&*C@&*+, (H%&(:6&H%&C@/96(@/@+, .*.0(
)SU(@+. %.(6&86.(@.(@8@+"@1+6(#%#%+(H%&(.69"&*#,(C%/*#%&*/I(F f&6II0(>?>?;KG5((
! (#&@96&9@++67(a1:H#&@96b(3@.(\$6(#%#%+(%H(9\$%*96(*/(:&68*%".(&6.6@&9\$(1,(- *+.%/(
F>?>?Y"/6G5(E#(*C:+*H*67(#\$6(3&*#*/I(@/7(@##@9\$C6/#(%H()SU(:&%I&@C.(1,(:&%8*7*/I(@/(
! - AQ+*N6(. ,/#@M'(
(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(|=(
!

!

(

```
#!/usr/bin/bpftrace  
  
probe1 /filter/ { action }  
probe2, probe3 /filter/ { action }
```

!

"#\$%&'!()*+,-./!0!123!-&.4'!

!

P\$6(#\$&66(C@*/(9% C: %/6/#.(%H(1:H#&@96(.,/#@M(@&6(#\$6(:&%160(#\$6(H*+6&0(@/7(#\$6(
@9#*%/5(P\$6(:&%16(.:69*H*6.(#\$6(#&@96:%*/#(%&(H"/9#*%/(3\$6&6(#\$6())SU(:&%I&@C(3*+(16(
@##@9\$670(#\$6(H*+6&(X"@+*H*6.(3\$*9\$(686/#.(@&6(:&%96..670(@/7(#\$6(@9#*%/(76H*/6.(#\$6(@9#*%/(
#%(#@N6(3\$6/(#\$6(686/(H*&6.5(

D69"&*#,(:&@9#*#*%/6&.(9@/(+686&@I6(1:H#&@96(%(@9\$*686(@&6C@&N@1+6(76:#\$(%H(
8*.*1*+*#,(%/ (L*/"M(.,.#6C.5(-*+.%/(F>?>?(Y"/6G(:&%8*767(1:H#&@96(.9&*:#.(#(76#69#(
9&,:#%9"&6/9,(.%H#3 @&6(#&@HH*90(:&%8*+6I6(6.9@+@*%/(@##6C:#.0/6#3 %&N(:*8%#(@##6C:#.0(
@/7(DDR(:&%M,(9&6@*%/(

[6.:*#6(*#. (1&%@7(C%/*%&*/I(9@:@1*+*#*6.0(1:H#&@96(3@.(+*C*#67(*/*#.(@1*+*#,(#%(
C*#*I@#6(@##@9N.5(!#(16.#0(#\$6(#%+(9%"+7(&6.:%/7(#%(@/(686/#(1,(.6/7*/I(@(. *I/@+(#%(@(
:&%96..(%&(1,("/.@H6+,(.:@3*/I(@(. \$6++(#%(:6&H%&C(@/(@9#*%/(Ff&6II0(>?>?D6:#6C16&G5(
- *+.%/(F>?>?(Y"/6G(9%/9+"767(#\$@#(H"#"&6(&6.6@&9\$(9%"+7(H%9".(%/ (ABDE0(@/("":Q

@/7Q9% C*/I(W!T(6M#6/.%/(#\$@#(3@.(16##6&(:%.*#*%/67(#%(C*#*I@#6(@##@9N.(3*#\$()SU5(
!"!\$ ()*+,\$- ./+0)12\$3 45+6.7\$

! /%#\$6&(6..6/#*@+(:&6&6X"*.*#6(#%(3&*#*/I(ABDE(:&%I&@C.(.*(" /76&.#@/7*/I(\$%3(
L*/"M(D69"&*#,(W%7"+6.(3 %&N5(W!T(6M#6/.%/(.*/(L*/"M(@&6(*C:+6C6/#67(@.(LDW.0(@/7(
#\$\$.(* /9+"76.(ABDE5(
P\$6(LDW(H&@C63 %&N(C@76(*#(:%..*1+6(#%(6M#6/7(#\$6(.69"&*#,(C%76+(%H(L*/"M(
3*#\$/(\$6(C@*/+*/6(N6&/6+5()6H%&6(*#.(6M*.#6/960(L*/"M(3@.(+*C*#67(#%([*.9&6#*%/@&,(
!996..(T%/%&+0(%&([!T(F) @&N+6,0;ZZ=G5(S&%069#.(#\$@#(@7767(W!T(%(L*/"M0(. "9\$(.(
W67".@0(BD) !T0([P^0(@/7(#\$6(_D!v.(D^L*/"M0(\$@7(#%(C@*/#*%/(#\$6*&(%3 /9".#%CQ
:@#9\$67(N6&/6+.(FDC@++6,0(>?>?(W@,G5(
@ 2021 SANS Institute Author Retains Full Rights

W**I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(J(

!

(

(

"#\$%&'!5)!6&'78*9!:&4;#-'4-%&'!-;.-!<'=%&'>!%?-0A!B'&,'!@!10&!9:?(

L*/"M(N6&/6+(C@*/#@*/6&.(686/#"@++,(9&6#67(#\$6LDW(H&@C63%&N(%(:&%8*76(@(
:@\$3@,(H%&(#\$6.6(9".#%C(.69"&*#,(:%069#.(#%(16(C6&I67(*/#%/#\$6(L*/"M(C@*/+*/6(N6&/6+(
FDC@++6,0(/575G5(W"+#*:+6(LDW.(36&6(686/#"@++,(C6&I670(1"#%/+,(%/6(%H(#\$6C(9%"+7(16(
6/@1+67(@#(@#*C65(

P\$6(#3%(1*II6.#(:+@,6&.(@C%/I(L*/"M(W!T(6M#6/.*%/.(36&6(D^L*/"M(H%&(B67(
R@#Q1@.67(7*.*&*1"#*%/.(@/7(!::!&C%&(H%&([61*@/Q1@.67(7*.*&*1"#*%/.(FDC@++6,0(>??>(
Y"/6()6@##60(>?;KG5(D^L*/"M(3@.(N/%3/(H%&(#, :6(6/H%&96C6/#0(3\$*9\$(6/H%&967(\$%3(
96&#@*/(#,:6.(%H(. "1069#.(9%"+7(*#6&@9#(3*\$(96&#@*/(#,:6.(%H(%1069#.5(!::!&C%&(##%N@/(
@+6&/@#6(@: :&%@9\$(%H(1@.* /I(*#.(:%+*9*6.(%/ (H*+6. ,.#6C(:@#\$\$.5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*\$(ABDE(|`(
!|

!

(

"#\$%&'!D)!8#,%/!*'4%&#-+!90>%^'@!:&4;#-'4-%&'(

P\$6&6(36&6(.686&@+(+6..6&QN/%3/(W!T(6M#6/.*%/.(@.(36++0(*9+"7*/I(DC@9N(
FT%%N0(>?;KG0(P]W]g](FP@N67@0(>??ZG0(@/7(g@C@(FT%%N0(>?;?G5()69@"6(%/+,(%/6(
LDW(9%"7(16(6/@1+67(@#(@#*C60(#\$6.6(.C@++6&(LDW.(36&6(%H#6/(9&%3767(%"#5(R%3686&0(
.#@&#*/I(*/>?;J0(C"+#*:+6(LDW.(9%"7(16(+@767(@#(#\$6(.@C6(#*C6(F^7I60(>?;JG5(
.

LDW(\$%N.(@&6(.#*+(\$6(9%CC%/(*/#6&H@96("67(1,(W!T(6M#6/.*%/5(P\$6,(@&6(
+*.#67(*/(\$6(L*/"M(N6&/6+(.%"&96(9%76(H*+6(a<*/9+"76<+*/"M<+.C2\$%%N276H.5\$5b(P\$6(
H%+%3*/I(@&6(@H63(6M@C:+6(6/#&*6.'(

```
LSM_HOOK(int, 0, inode_permission, struct inode *inode, int mask)
LSM_HOOK(int, 0, bprm_check_security, struct linux_binprm *bprm)
LSM_HOOK(int, 0, socket_listen, struct socket *sock, int backlog)
```

(

"#\$%&'!E)!F/4'&3-!0!G#,4C%>'G0#,%/G0@AH;00IH>'1@);(

P\$6(LDW2R]]AFG(C@9&%(.:69*H*6.(\$6(H"/9#%*/(&6#"&/(#,:60(\$6(76H@"+#(&6#"&/(
8@+"60(\$6(/@C6(%H(\$6(.69"&*#,((\$%%N0(@/7(\$6(+*.#(%H(@&I"C6/#.(:@..67(*/%#(\$6(\$%N5(
.

P\$6(H*&.#(+*/6(%H(\$6(6M96&:#@1%86*(.H%&(@(\$%%N(/@C67(*/%762:6&C*..*%/5(E#.(
@&I"C6/#.(@&6(@/(*/%76(.#&"9#"&6(F3\$*9\$(9%/#@*/.(\$6(C6#@7@#@(H%&(@H*+6G(@/7(@/(*/#6I6&(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(| K(

!
#\$@#(&6:&6.6/#.(#\$6(:6&C*..%/(C@.N5(- \$6/(@/(LDW(\$%%N*(.##*II6&670(9%/##%+(*.(:@..67(##(
%/6(%&(C%&6(LDW.(3\$*9\$(6M@C*/6(\$6(@&I"C6/#.(:@..67(##(\$6(\$%%N(@/7(\$6/(@++3(%&(

! /%#\$6&(L*/"M(N6&/6+(.% "&96(H*+6."::+6C6/#.(* /H%&C@#%/(@1%"#(\$6.6(\$%%N.5(P\$6(
H%+3*/I*(.(@/(6M96&:#(H%&C(a<*/9+"76<+*/"M<+.C2\$%%N.5\$b(@1%"#(\$6(*%762:6&C*..%/(
\$%%N0(.+*I\$#+, (C%7*H*67(H%&(&6@7@I*+##, '(

```
* @inode_permission:  
*   Check permission before accessing an inode.  
*   ...  
*   @inode contains the inode structure to check.  
*   @mask contains the permission mask.  
*   Return 0 if permission is granted.
```

(
"\$%&'!J)!F/4'&3!O!G#,4C%>'C%#,%/C@AH;OOI@);(

P\$*(6/#&,(7%9"C6/#.(#\$@#(\$6(*%762:6&C*..%/((\$%%N(9@/(16("67(H%&(&77*#%/%@+(
:6&C*..%/(9\$69N.(16H%&6(@++3*/I(@996..(##(@/(/*%765(D69"&*#,(:&@9*#%/%6&.(9@/(
&6H6&6/96(\$6.6(#3%(.% "&96(H*+6.(##(" /76&.#@/7(\$6(: "&: %.6(@/7(" .@I6(%H(686&,(LDW(\$%%N(
/(\$6(L/"M(N6&/6+5(P\$6,(9@/(16(8*6367(%/+*/6(3*#\$(#\$6(^+M*&(T%&..(B6H6&6/96&(@#(
\$##:.'<<6+*M*&51%%%#+/59% C5(

7#!8/'%/1!4*%&,9/!:/+*','&3!\$%;&'*9/%&<&,(%!

E/(D6:#6C16&(>?;Z0(AS(D*/I\$(:&:%.67(@(.6#(%H(N6&/6+(:@#9\$6.(##(\$6(L*/"M(
A6&/6+(W@*+*/I(L*.#(H%&(@(/63(LDW(9@++67(aA6&/6+(B"/#*C6(D69"&*#,(E/.##"C6/#@#%/%0b(%&(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(| h(

!

(

"#\$%&'!K)!L@#,\$!8*9!M00I@!N#;!B<*0(

P\$6(:@#9\$6.(36/#(\$%&"I\$(.686&@+(&68*.*%/.(@/7(36&6(C6&I67(*/#%(\$6(C@*/*+*/6(
L*/"M(N6&/6+*/(W@&9\$(>?>?(F)%&NC@//0(>?>?G5(P3%(C%/#\$.(+@#6&0(L*/"M(N6&/6+(86&.*%/(
J5K(3@.(\$6(H*&.#(#%(*+/"76(ABDE0(&6+6@.67(%/(c;(W@,(>?>?(FT%&16#0(>?>?(Y"/6G5(

ABDE(:&%I&@C.(@&6(16*/I(".67(*/(:&%7"9#*%/(@#(f%%I+6(H%&(C*#*I@#*/I(8@&*%".(
@##@9N.0(*+/"7*/I(L[2SB^L]![(@##@9N.(FD*/I\$0(>?;Z([696C16&G5(

e/H%&#" /@#6+,0(3%&N*/I(6M@C:+6.(%H(".* /I(ABDE*/(\$6(C@*/*+*/6(N6&/6+(@&6(@+C%.#(
/%/Q6M*.#6/#5(P\$6(6M@C:+6.(*+/"767(*/(\$6(ABDE(:@#9\$6(.6#(76:6/767(%/(.:69*@+(\$6+:6&(

8"#"\$ 94467\$:40\$; 0)1)*<\$=> -?&\$04<0@A7\$

P\$6&6(@&6(\$&66(C@*/(%%+.6#. (H%&(3&*#*/I())SU(:&%I&@C.'(1:H#&@960(\$66())SU(
T% C:*+6&(T%++69#*%/(F)TTG0(@/7(\$66())SUQ&6+@#67(%%+.(:&%8*767(*/(\$6(L*/"M(N6&/6+(

P\$6(C%.#(@: :&%@9\$@1+6(%H(\$66(\$&66(%%+.(*(1:H#&@960(1"#(*#(7%6.(/%#(.": :%&#(ABDE(
,6#5(P\$6&6*.(@(: "+&6X"6.#(H%&(\$*.(H6@#"&60(1"#(*#(\$@.(/%#(166/(C6&I67(,6#(7"6(#%(*#.(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(Z(

!
76:6/76/9,(%/(@C*..*/I(N6&/6+(\$6+:6&(H"/9*%/(F]+. @0(>?>?G5(] /96(#\$6(: "+(&6X"6.#*(.
C6&I670(3 &*#*/I(ABDE(:&%I&@C.(3*++(169% C6(C"9\$(*C:+6&5(P\$6(H%++%3*/I(*.(@1@.*9(
6M@C:+6(%H(".* /I(1:H#&@96(%(+%@7(@ (ABDE(:&%I&@C(#\$@#(:&686/#.(@ / ,(%#\$6&())SU(:&%I&@C.(
H&%C(16*/I(+@767'(

bpfttrace -e 'lsm:bpf { return -1234; }'

(
"\$%&'!P)!F/ . A3\ '!0!%@# , \$!B< *0!N#- ;!231-& .4' (

P\$*.(:&%I&@C(@##@9\$6.(#%(\$6(a1:Hb(LDW(\$%N0(3\$*9\$(:6&H%&C.(#\$6(*/*#*+@9\$69N(
H%&(@++(1:HFG(. ,.9@++5E#(%86&&*76.(#\$6(&6#"&/ (8@+"6(3*#\$(@(/%/Qd6&%(*/#6I6&0(9@".* /I(@++(
H"#"&6(@##6C:#.(#%(9@++(1:HFG(#(H@*+("/#*+(\$6(:&%I&@C(*.("/+@7675(E/(%#\$6&(3%&7.0(#\$*.()SU(
: &%I&@C(1+9N.(%#\$6&())SU(:&%I&@C.(H&%C(+@7*/I5(
(P\$6(.69%/7(#%%+(%H(9\$%*96(*.()TT5(U%&#" /@#6+,0(*#(\$@.(." : :%C(ABDE(* /96(*#.(
?5;J5?(&6+6@.6*(/Y"/6(>?>?FD%/I0(>?>?G5(!.(."9\$0(\$\$*.(&6.6@&9\$(3*++(&6+,(%/()TT5(
- &*#*/I()TT(.9&*:#.(.*I/*H*9@/#+, (C%&6(* /8%+867(\$@/(3&*#*/I(1:H#&@96(.9&*:#.5(
P\$6&6(@&6#3%(\$@+86.(#%(6@9\$())TT(.9&*:#(\$6(H*&.#(\$@+H*.(#\$6())SU(:&%I&@C(#\$@#(3*++(16(
+%@767(* /#%(N6&/6+Q. : @965(P\$*.(:%&#*%/(*(.(3&*#6/(*/(T5(P\$6(.69%/7(\$@+H(*.(#\$6(" .6&Q. : @96(
.9&*:#(\$@#(3*++(+@7(\$6())SU(:&%I&@C0(:%++(7@#@ (H&%C(*#@/@7(H@9*+*#@#6(8@&*%".(9%CC@/7Q
+*/6(:%#*%/.5(P\$*.(:%&#*%/(*(.(3&*#6/(*/(S, # \$ % /5(P\$6(S, # \$ % /(.9&*:#(9@/(6*#\$6&(6C167(#\$6(T(
: &%I&@C(3*#\$/(*#%&(&6H6&6/96(*#@.(@(.6: @&@#6(H*+65(! (H"+(#"%&*@+(H%&(&3&*#*/I(@1@.*9())TT(
.9&*:#(9@/(16(H%"/7(* /(! : :6/7*M(!5(
=#!>%<13; , ; ! (?!84 : \$! , ! @AB!

(P\$6(&6C@*/76&(%H(\$\$*.(: @ :6&(*.(767*9@#67(#%(C6@."&*/I(\$6(@1*+*#,(%H(ABDE(
: &%I&@C.(#%(C*#*I@#6(@##@9N.(*/(@/(RST(6/8*&%/C6/#5(! (#6.#(6/8*&%/C6/#(3@.(1"*+*#(#(
9% C : @&6(\$6(H"/9*%*/@+*#,(@/7(:6&H%&C@/96(%H(ABDEQ7*.@1+67(@/7(ABDEQ6/@1+67(. , .#6C.5(
B"#"\$ => - ?\$ - /0)C17\$

U*86()TT(.9&*:#.(3&6&(3&*#6/(\$@#(" .67(ABDE(H%&(C@/7@#%&,(@996..(9%/#&%+5(
P\$6*&(. "%&96(9%76(*.(@8@*+@1+6*/(@(: "1+*9(f*#R"1(&6:%(F - *+.%/0(>?>?(]9#%16&G5(P\$6(
.9&*:#.(3&6&(3&*#6/(\$@#(77&6..(\$6(H%++%3*/I(X"6.#*%/. '(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(;?(!

!

- ! T@/(ABDE(1+%9N(@/7(&6: %&#(" .6&.(3\$(9&6@#6(H*+6.(3*\$(*/.69"&6(:6&C*..%*/.i(
- ! T@/(*(1+%9N(@/7(&6: %&#(" .6&.(3\$(%&#("/("/@#"#\$%&*d67(6M69"#@1+6.i(
- ! T@/(*(1+%9N(@/7(&6: %&#(" .6&.(3\$(6.#@1+*.\$(DDR(:&%M*6.i(
- ! T@/(*(1+%9N(@/7(&6: %&#(" .6&.(3\$((:*8%#%#("/@#"#\$%&*d67(/6#3%&N(.6IC6/#.i(
- ! T@/(*(1+%9N(@/7(&6: %&#("/@#"#\$%&*d67(@##6C: #.(#%(#6&C*/@#6(:&%96..6.i(

! ++(\$6(.9&*: #.(+ %II67(686/#(7@#@(&6I@&7*/I(\$6(:&%96..6.(\$@#(9@" .67(\$6C(#(H*&65(P\$*. (7@#(*/9+"767(\$6(#*C6.#@C: 0(9%CC@/7(/@C60(eE[0(fE[0(@/7(SE[(%H(\$6(:&%96..6.0(@.(36++(@./, (@9#%*/. (#@N6/(F@++% 3(%&(76/, G5(^@9\$(.9&*: #(@+. %(&69%&767(@77*#%*/@+(7@#(#\$@#(3@. ("/*X"6(#%(\$6(#, :6(%H(686/#(\$@#(*#(\$@/7+675(P\$6(.9&*: #.(3&%#6(+%I. (*/(N6, Q8@+"6(H%&C@#0(1"#H%&(\$6(H%++% 3*/I(.69#%*/.0(\$6(+%I.(36&6(@70".#67(#%(@(\$6@76&Q9+"C/(H%&C@#(3*\$(@(#&"/9@#67(#*C6.#@C: (H%&(&6@7@1*+*, 5(

!"#"\$%&'()*+, - , .%/ \$

P\$6(C@92H*+6:6&C.(.9&*: # (3@.(3&*#6/(#%(&6.#&*9#(" .6&.(H%&C(.6##*/I(\$6(DeE[(FD6#(eE[G(@/7(-] PR(F - &*#@1+6(1, (] # \$6&.G(:6&C*..%*/(1*#.(%H(H*+6.5(

P\$6(DeE[(@/7(-] PR(1*#.(@&6(+6I*#*C@#6(9% C: %/6/#.(%H(\$6(L*/"M(:6&C*..%*/.(C%76+(\$@#(@&6(N/% 3/(#%(16(@1".67(1, (@##@9N6&.5(D6##*/I(\$6(DeE[(1*#%/(@H*+6(3*+(@++% 3(@(" .6&(#(6M69"#6(*#(3*\$(#\$6(H*+6(% 3/6&V. (:&*8*+6I6.5(E#(*./696..@&, (H%&(6M69"#@1+6.(+*N6(a:@..37b(@/7(a."7%0b(1"#(C@+*9%". (:&%I&@C.(\$@86(@+. %(.6#(\$6(DeE[(1*#%/(H*+6.(#(C@*/#@*/(:6&*. #/6#(1@9N7%&.(FWEPB^0(>?>?(!"I".#G5(P\$6(-] PR(1*#(@++% 3.(@/, %/6(#%(3&*#6(#%(@I*86/(H*+65(E#(*.%H#6/(.6#*/9%&&69#+, (1, (" .6&.(#%(6/. "&6(@/(@: :+*9@#%*/(3%&N.(FWEPB^0(>?>?(W@&9\$G(%&(#%(*/#6/#%*/@++, (. \$@&6(7@#@ (3*\$(:66&.5(W@+*9%". (@9%&.(9@/(H*/7(@/7@1".6(H*+6.(\$@#(@&6(3&*#@1+6(1, (@/, %/65(

P\$6(C@92H*+6:6&C.(.9&*: #(@##@9\$67(:&%I&@C. (#%(\$6(a*/%7629&6@#6b(@/7(a:@#\$29\$C%7b(LDW(\$%N.5(P\$6.6(\$%N. (36&6(#&*II6&67(3\$6/(@/63(H*+6(3@.(9&6@#67(%&(@/6M*.*#/I(H*+6V. (:6&C*..%*/.(36&6(C%7*H*670(&6.:69#*86+, 5(

P\$6(@##@9\$67(:&%I&@C. (:&686/#67(DeE[(@/7(-] PR(:6&C*..%*/(1*#.(H%&C(16*/I(.6#%/(/63(H*+6. (%&(@7767(#%6M*.*#/I(H*+6.5(E#(7*7(.%1, (6M@C*/*/I(\$6(&6X"6.67(:6&C*..%*/.(C%76(%H(@H*+6(@/7(\$6("C@.N(%H(\$6(:&%96..5(EH(*#(76#69#67(@DeE[(%&(-] PR(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*#\$(ABDE(|; ;(
!

1*#(&6X"6.#0(#\$6/(#(9%" +7(:&686/#(#\$6(H*+6(H&%C(16*/I(9&6@#67(%&(#\$6(H*+6(:6&C*..*%/.(H&%C(
16*/I(" :7@#675(

U*I"&6(h(16+%3(.\$%3.(@/* /8%9@#*%/(%H(#\$6(C@92H*+6:6&C.(.9&*:#(@/7(*#.(&6."+#@/#(
6HH69#(%/(#\$6(" .6&(a1*++,0b(3\$%(\$@.(eE[(;???)5(

E/8%9@#*%/(%H(C@92H*+6:6&C.'										
# ./mac_fileperms -D -u billy										
TIMESTAMP	TYPE	COMM	UID	GID	PID	OLDMOD	REQMOD	UMASK	NEWMOD	ACT
T13:09:34	chmod	chmod	1000	1000	18064	100664	-	-	004664	deny
T13:09:59	creat	touch	1000	1000	18073	000000	100666	000000	100666	deny
T13:11:10	chmod	chmod	1002	1002	18163	100664	-	-	004664	allow
T13:11:42	creat	touch	1002	1002	18168	000000	100666	000000	100666	allow
e.6&(#6&C*/*+!'										
billy@linux1 ~ \$ touch /tmp/suidfile										
billy@linux1 ~ \$ chmod u+s /tmp/suidfile										
chmod: changing permissions of '/tmp/suidfile': Operation not permitted										
billy@linux1 ~ \$ umask										
0002										
billy@linux1 ~ \$ umask 0000										
billy@linux1 ~ \$ touch /tmp/writable-by-others										
touch: setting times of '/tmp/writable-by-others': No such file or directory										
billy@linux1 ~ \$(

(
"\$%&'!Q)!0,R04.-#0,!.,>!F11'4-!0!SA.4H1#0'3'&A@T(

P\$*.(.9&*:#(3@.(*/8%N67(*/([6/, (W%760(.:69*H,*/I(\$@#(#\$6(" .6&(a1*++,b(.\$%" +7(16(
1+%9N67(H&%C(@77*/I(DeE[(%&(-] PR(:6&C*..*%/(1*#.0(3\$6#\$6&(#\$&%" I\$(H*+6(9&6@#*%/(%&(
H*+6(C*7*H*9@#*% /5(] #\$6&(" .6&.(36&6(/%#(&6.#&*9#675(

P\$6(" .6&(a1*++,b(@##6C:#67(#%(@77(DeE[(:6&C*..*%/(1*#.(#%(@ (H*+60(1"#/9\$C%7(
&6#"&/67(@/(6&&%&5((P\$6(" .6&(#\$6/(9\$@/ I67(#\$6*&(. \$6++V.(" C@.N(#%(* /9+"76(#\$6(-] PR(1*#(H%&(
/63+, (9&6@#67(H*+6.5(- \$6/(\$6(" .6&(&@/(\$6(#% "9\$(9%CC@/7(#%(9&6@#6(@ (H*+6(3*#(\$66(
-] PR(1*#(.6#0(\$6(9%CC@/7(H@*+67(#%(9&6@#6(\$6(H*+65(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*#\$(ABDE(|;c(

!

E/8%9@#*%/(%H(C@92."*76M69'(
# ./mac_suidexec -D -u billy -F /bin/passwd									
T14:48:15	exsuid	bash	1000	1000	21307	42	43091310	104755	allow
T14:48:22	exsuid	bash	1000	1000	21317	42	43091340	104111	deny
T14:48:30	exsuid	bash	1000	1000	21325	42	43091580	104755	deny
e.6&(#6&C*/@+ '!									
billy@linux1 ~ \$ passwd									
Changing password for user billy.									
Current password: ^C									
billy@linux1 ~ \$ sudo -i									
-bash: /bin/sudo: Operation not permitted									
billy@linux1 ~ \$ newgrp									
-bash: /bin/newgrp: Operation not permitted!									

(

"#\$%&'!U)!0,R04.-#0,!.,>!F11'4-!0!\$A.4H@%#>'/'4T(

(P\$6(@1%86(* /8%9@#*%/(%H(C@92."*76M69(:&686/#67(#\$6(" .6&(a1*++,b(H&%C(* /8%N* /I(@ / ,(DeE [(1* /@&*6.(%/ (#\$6(.,.#6C()41)50(H%&<1* /<:@...37(F.*I/*H*67(1,(#\$6(9@: *#@+(QU(%: #*% /G5(- \$6/ (#\$6(" .6&(@##6C: #67(#%&" / (#\$6(a: @...37b(1* /@&,0(*#(."99667675(R%3686&0(@##6C: #.(#%&" / (a."7%b(@ /7(a/63 I&: b(36&6(1+%9N67(@ /7(+%II67(1,(#\$6(.9&*: #5(P\$6(.9&*: #(+%II67(#\$6(686/#(#, :6@.(a6M."*7b(@ /7(&69%&767(#\$6(H*+6V.(*/%76(/ "C16&0(768*96(/ "C16&0(@ /7(C%765(P\$6(.9&*: #(&@9N67(H*+6.(1,(*/%76(@ /7(768*96(/ "C16&.(&@#\$6&(#\$@ /(: @#\$\$.5(

!"#4"\$ %&' (//5+ /6,7, . /\$

P\$6(C@92..\$+.#6/6&.(.9&*: #(:&686/#67(#\$6(9&6@#*%/(%H(DDR(:&%M,(#" / /6+.(@ /7(\$@ /7+67(1%#\$ (ES8=(@ /7(ES8` (@77&6..6.5(

E/(aD69"&* /I(#\$6(D%H#(e /76&16++,(%H(@D":6&9%C:"#6&(3*#\$() SU(S&%16.0b(- *+.% / (F>?>?(Y" /6G(1&*6H+, (6M: +@* /67(PTS(:%&#(H%&3 @&7* /I5(E#(*.(@ (1"*+Q* / (DDR(H6@#" &6(#\$@#(@++3.(.%C6%/6(#%(" .6@(.6&86&(@.(@(:&%M,(#%(&6@9\$(6M#6& /@+(&6.% "&96.5(P\$*.(H6@#" &6(9@ / (16(".67(#%&#&@ / .H6&(7@#@(#%(@ /7(H&%C@ (768*96(#\$@#(+@9N.(7*&69#(@996..(#%(\$6(* /#6& /6#5(!+#\$%" IS(#\$6(H6@#" &6(9@ / (16(7*. @1+67(% / (DDR(.6&86&.0(*#(*.(%/ (1,(76H@ "+"@ /7(" ."@++,(+6H#(

P\$6(H%+% 3*/I(3@.(@/(/*8%9@#*%/(%H#\$(C@92..\$+*.#6/6&.(.9&*:#(@/7(*#.6HH69#(%/(@(" .6&(3\$(@##6C:#67(#(%:#/(@/(DDR(:&%M,("#//6+5()6H%&6*(8%N*/I#\$(.9&*:#0(#\$6(@""#\$%&(.+*I\$#+, (C%7*H*67(*#(%(&6#"&/(\$6(Q_]LE_A(6&&%&(":%/(76/*@+(*/.#6@7(%H#\$(Q^S^BW(6&&%&5(P\$*.(3@.(7%/6(%(76C%/ .#&@#6(\$@#(#\$6.6(.9&*:#.9@/(&6#"&/(@&1*#&@&,(6&&%&8@+"6.(#(%#\$6(" .6&5(

```
E/8%9@#*%/(%H(C@92..$+*.#6/6&.'(
# ./mac_sshlisteners -D -U root
TIMESTAMP TYPE COMM UID GID PID PROTO LADDR LPORT ACTION!
T08:53:39 listen ssh 1000 1000 6602 6 [::1] 9999 deny!
T08:53:39 listen ssh 1000 1000 6602 6 127.0.0.1 9999 deny
e.6&(#6&C*/@+!
billy@linux1 ~ $ ssh -D 9999 10.7.7.6!
listen: Link has been severed!
listen [::1]:9999: Link has been severed!
listen: Link has been severed!
listen [127.0.0.1]:9999: Link has been severed!
channel_setup_fwd_listener_tcpip: cannot listen to port: 9999!
Could not request local forwarding.!
Last login: Thu Oct 8 16:49:11 2020 from 192.168.100.15!
billy@login1
```

P\$6(.9&*:#(3@.*/8%N67(*/([6/ ,(W%76(3*#\$(@9@:*#@+aQ e b(#%(76/ ,(@++(" .6&.(6M96:#(&%%#(H&%C(% :6*/I(:&M.("#"/+.(3*#\$(DDR(9+*6/#.5)P\$6(" .6&(#\$6/(@##6C:#67(#(% :6/(@/(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(;J(!

! DDR(:&%M,(#"//6+(3*\$(7,/ @C*9(:%&#(H%&3@&7*/I(F.*I/*H*67(1,(#\$6(DDR(9+*6/#V.(Q I (%:#*%/G5(- \$6/(#\$6(9+*6/#(@##6C:#67(##(9\$@/I6@/(ES8`(.%9N6#(##(#+*.#6/*/I(.#6#6(#+%9@+(:%&#(ZZZZ0)*#(3@.(I*86/(#\$6(6&&%&(\$#@#(#+*/N(3@.(.686&675(E#(\$6/(@##6C:#67(@/%#\$6&(+*.#6/(%:6&@#*%/(3*\$(@/(ES8=(.%9N6#0(3\$*9\$(H@*+67*/(\$6(.@C6(C@//6&5(P\$6(DDR(9%/ /69#*%/(#% (\$6&6C%#6(\$% .#(.#*+ (. "9966767(H%&(\$6(" .6&0(1"#(\$6(:&%M,(#"//6+(3@.(/%#(. "996..H"++,(6.#@1+*.\$675(P\$6(.9&*:#(+%II67(1%#\$(#\$6(ES8=(@/7(\$6(ES8`(@##6C:#.(##(9\$@/I6@(.%9N6#(##(@ +*.#6/*/I(.#@#65(

!"#!"\$%&'(/8'977,'6*97/\$

P\$6(C@92.N9%/ /69#*%/.(.9&*:#(&6.#&9#67(.%9N6#(9%/ /69#*%/.(##(96&#&@*/(76.#*/@#*%/.5(E#(\$@7(H"++(8*.1*+*#,(*/#%(@/,(.%9N6#(9%/ /69#*%/(@##6C:#0(1"#*#(3@.(3&*##6/(#% (%/+,(6M@C*/6(ES8=(.%9N6#(9%/ /69#*%/.(H%&(\$*\$.(&6.6@&9\$5(P\$*.(9&*:#(:&%#69#67(@I@*/.#(:*8%#(@##6C:#.(1,(@77*/I(:6&Q".6&(H*63@++(&6.#&9#*%/.0(@/7(*#(7*7(.%(3*#\$%"#(C*7*H,*/I(#\$(6(\$% .#V.(96/#&@+(H*63@++(9%/H*I" &@#*%/5(

P\$6(.9&*:#(3@.(86&,(.*C*+@&#%(@())SU(#&@9*/I(.9&*:#(" .67(1,(- *+.%/(F>?>(Y"/6G(9@++67(#9:29%/ /69#H*+6&5.\$5(P\$*.(9&*:#(%/+,(\$@/7+67(PTS(9%/ /69#*%/.(8*@\$6(#9:29%/ /69#FG(N6&/6+(H"/9#*%/0(@/7(*#(3@.(+*C*#67(##(76#69#*%/5(E/(9%/#&@.#0(\$6(C@92.N9%/ /69#*%/.(.9&*:#(\$@/7+67(@/, (ES8=(.%9N6#(9%/ /69#*%/.(&6I@&7+6..(%H(\$6("/76&+,*/I(:&%#%9%+0(@/7(*#(:&%8*767(1%#\$(76#69#*%/(@/7(C*#*I@#*%/5(

P\$6(C@92.N9%/ /69#*%/.(.9&*:#@##@9\$67(@(:&%I&@C(##(\$6(a.%9N6#29%/ /69#b(LDW(\$%%N0(3\$*9\$(H*67(3\$6/(@(:&%96..(@##6C:#67(##(C@N6(@(.%9N6#(9%/ /69#*%/5(P\$6(H%++3*/I(3@.(@/(6M@C:+6(%H*/8%N*/I(\$6(C@92.N9%/ /69#*%/.(.9&*:#(@/7(\$%3(*#(HH69#67(@(" .6&5(

(
(
(
(
(
(
(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*#\$(ABDE(|;`(!

!

E/8%9@#*%/(%H(C@92.N9%/ /69#*%/.'(
# ./mac_skconnections -D 10.100.0.0 -m 255.255.0.0 -u billy									
T10:45:00	skconn	ssh	1000	1000	10109	6	10.100.3.4	22	deny!
T10:45:11	skconn	ssh	1000	1000	10160	6	10.101.3.4	22	allow!
T10:50:02	skconn	dnf	0	0	10275	17	10.102.5.6	53	allow!
T10:50:02	skconn	dnf	0	0	10275	6	209.132.183.108	443	allow!
T10:51:57	skconn	nc	1002	1002	10357	6	10.100.10.11	80	allow!
T10:57:20	skconn	nc	1000	1000	10644	17	10.102.5.6	53	deny
e.6&(#6&C*/*+!									
billy@linux1 ~ \$ ssh 10.100.3.4									
ssh: connect to host 10.100.3.4 port 22: Operation not permitted!									
billy@linux1 ~ \$ ssh 10.101.3.4!									
Last login: Fri Oct 9 16:46:37 2020 from 192.168.10.15!									
billy@login3 ~ \$ ^C!									
billy@linux1 ~ \$ nc -u 10.100.4.5 53!									
Ncat: Operation not permitted.									

(

"#\$%&'!()!0,R04.-#0,!. ,>!F11'4-!0!\$A.4H@!40,, '4-#0,@T(

P\$6(.9&*:#(3@.(*/8%N67(#(1+%9N(#\$6(" .6&(a1*+,b(H&%C(C@N*/I(ES8=(. %9N6#(9% / /69#*% / .(#%(\$6(; ?5; ??5?5?<; `(."1/6#(- \$6/(\$6(" .6&(@##6C:#67(#(DDR(#(@/76.#*/@#*%/(*/(\$#@#("1/6#(\$6(%:6&@#*%/(3@.(/%#(:6&C*##675(P&,*/I(@/%#\$6&(76.#*/@#*%/(%"#. *76(#\$6(&6.#&*9#67(. "1/6#(3@.(."996..H"+5(P\$6(.9&*:#(\$6/(+%II67(.%C6(.%9N6#(9% / /69#*% / .(1,(\$6(.6&86&V.(:@9N@I6(C@/@I6&0([@/7*H*67(g e W(F7/HG5(P\$6.6(9% / /69#*% / .(3 6&6(@++3 675(P\$6(" .6&(#&*67(@H*/@+(/69#@#(#%(; ?5; ??5=5J(%/(:%&#(Jc0(3 \$*9\$(3 @.(1+%9N67(1,(\$6(.9&*:#5(

!"#": "\$ %&' (8*+6&/8/\$

P\$6(C@92N*+##@.N.(.9&*:#(&6.#&*9#67(:&%96..(*I/@+.5(E#(3@.(".67(#(:&%#69#(@+(\$6() TT(.9&*:#.(H&%C(6@&+,(#6&C*/*#*% /0(3 \$6#\$6&(1, (" / :&*8*+6I67(" .6&.(%&(&%#5(E#(\$@/7+67(% /+, (DE f AELL(@/7(DE f P^BW(*I/@+.0(1"#(*#(9%" +7(16(6M#6/767(#%(\$@/7+6(@/ ,(. *I/@+5(

D6/7*/I(*I/@+.(*(@H"/7@C6/#@+(:@&#(H(L*/"M(@/7(%#\$6&(S] DE j (%:6&@#*/I(., #6C.5(D*I/@+.(9@/(*/H%&C(:&%96..6.(#\$@#(@/(686/#(\$@.(%99"&&67(FA6&&*.NG5(P\$6,(9@/(@+.(%(:@".6(%&(#6&C*/*#6(:&%96..6.5(P\$6(N6&/6+I6/6&@#6.(#\$6C0(1"#(%#\$6&(. ,. #6C(:&%96..6.(9@/(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(;K(

!
&6X"6.#(#\$@#(#\$6(N6&/6+(.6/7(. *I/@+. (%/(\$6*&(16\$@+H5(] 86&(#\$*&#,(. *I/@+. (@&6(@8@*+@1+6(%/(
L*/"M0(1"#(#\$6(#3%(&6.#&*9#67(1,(\$*.(.9&*:#(36&6(DE f P^BW(F@.N(@(:&%96..(%(#6&C*/@#6(
#.6+HG(@/7(DE f AELL(FN+(\$6(:&%96..(*CC67*@#6+,G5(

P\$6(H%++3*/I*(.(@/(6M@C:+6(%H*/8%N*/I(C@92N*++@.N.(#(:&%#69#(@/(*/.#@/96(%H(
C@92H*+6:6&C.(@/7(*#. (6HH69#(%/(\$6(&%%#(" .6&5(

E/8%9@#*%/(%H(C@92N*++@.N. '(
# ./mac_fileperms -A -u root &									
[2] 18290									
# mac_fileperms_pid=\$!									
# ./mac_killtasks -D -e -t \$mac_fileperms_pid									
TIMESTAMP	TYPE	COMM	UID	GID	PID	TARGETUID	TARGETPID	SIGNO	ACT
T14:36:13	sgkill	bash	0	0	11342	0	18290	15	deny
T14:36:17	sgkill	bash	0	0	11342	0	18290	9	deny
T14:36:32	sgkill	bash	0	0	11342	0	18316	9	deny
T14:36:44	sgkill	bash	0	0	11342	0	18399	15	allow
!(&%%#(#6&C*/@+!									
# pgrep -fl mac_									
18290 mac_fileperms									
18316 mac_killtasks									
# kill 18290									
-bash: kill: (18290) - Operation not permitted									
# kill -9 18290									
-bash: kill: (18290) - Operation not permitted									
# kill -9 18316									
-bash: kill: (18316) - Operation not permitted									
# sleep 1000 &									
[1] 18399									
# kill 18399									

(
"#\$%&'!(5)!0,R04.-#O,!.,>!F11'4-!0!SA.4HI#00-.@I@T(

P\$6(.9&*:#(\$%%N67(*/#%(\$6(a#@.N2N*+b(LDW(\$%%N0(3\$*9\$(H*&67(3\$6/(@(. *I/@+(3@.(
@1%"#(#%(16(.6/#(#%(@(:&%96..5(E#(6M@C*/67(#\$6(@##&*1"#6.(%H(#\$6(.%"&96(:&%96..(@/7(#\$6(
#@&I6#(:&%96..(%(76#6&C*/6(3\$6#\$6&(\$6(. *I/@+(\$%" +7(16(@++367(%&(/%#5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(| ;h(!

!

(U*&.#0(C@92H*+6:6&C.(3@.(*/8%N67(#%(@++ 3%/+,(\$6(&%%#(" .6&(#%9&6@#6(H*+6.(3*\$(DeE[(%&(-]PR(1*#.5(P\$6(:&%96..E[(%H(\$@#(.9&*:#(3@.(. @8675(P\$6/(C@92N*++@.N.(3@.(*/8%N67(.%(\$@#(/%(:&%96..6.(9%" +7(.6/7(N*+(*I/@+.(#%(\$6(C@92H*+6:6&C.(:&%96..(%&(#%(\$6(C@92N*++@.N.(:&%96..(\$@#(:&%#69#67(*#5(

E/(@/%#\$6&(#6&C*/@+0(\$6(&%%#(" .6&(+%%N67(" :(\$6(SE[(.%H(\$6(#3%(.9&*:#.(@/7(@##6C:#67(#%(.6/7(@DE f P^BW(*I/@+(\$6(C@92H*+6:6&C.5(P\$*.(@##6C:#(H@*+675(P\$6(&%%#(" .6&(\$6/("/. "996..H"++,(##6C:#67(#%(.6/7(DE f AELL(*I/@+.(#%(1%\$\$() TT(.9&*:#.5(P\$6.6(@+.(H@*+675(U*/@++ ,0(&%%#(. :@3/67(@(.+66:(:&%96..(@/7(.6/#(*#@DE f P^BW(*I/@+5(P\$*.(."9966767(@/7(@++@9#8*#*6.(36&6(+%II675(

P\$6(.9&*:#(:&%8*767(#3%(/63(% :#*%/. 'QQN6&/6+(FQNG(@/7(QQ6#6&/@+(FQ6G5(P\$6(QQN6&/6+(% :#*%/(C%7*H*67(\$6(@##@9\$67(:&%I&@C(%(@+.%9%/##%+(*I/@+.(%&*I*/@##/I(H&%C(\$6(N6&/6+(*#.6+H*/(@77*#*%/(#%(\$% .6&6X"6.#67(1,(" .6&Q.:@96(:&%96..6.5(P\$*.(@"#\$%&(7*7(/%#(#6.#(\$6(*C: +*9@#*%/.(%H(1+9N*/I(*I/@+.(H&%C(N6&/6+Q.:@96(:&%96..6.(@/7(\$6&6H%&6(C@N67(\$\$*.(% :#*%/(@.(a7@/I6&%" .b*/(\$6(.9&*:#V.(\$6+:(#6M#5(P\$6(QQ6#6&/@+(% :#*%/(6/. "67(\$@#(\$6(C@92N*++@.N.(6M69"#@1+6(*#.6+H(3@.("/N*++@1+6(1,(@/ ,(:&%96..(6M96:#(H%&(*#.(:@&6/#(:&%96..5(EH(\$6(:@&6/#(:&%96..(6M*#670(/%#\$*/I(9%" +7(N*+(\$6(:&%96..5(

B"!\$ 9.71\$D*E)04*A.*1\$

P3%(L*/"M(N6&/6+.(36&6(9% C:*+67(\$@#(7*HH6&67(%/+,(*/(3\$6#\$6&(ABDE(3@.(6/@1+67(%&/%#5(k6&.*%/(J5h5;?(%H(\$6(.%"&96(9%76(3@.(".670(3\$*9\$(3@.(#\$6(C%.#&696/#(#@1+6(86&.*%/(@8@*+@1+6(@.(%H(>;(D6:#6C16&(>?>?5((

P\$6(L*/"M(N6&/6+.(36&6(9%/H*I"&67(@.(.*C*+@&+,(@.(:%..*1+6(#%(\$6(N6&/6+(\$@#(*.(*/9+"767*/(B67(R@#(^/#6&:&* .6(L*/"M(7*.#&*1"#*%/.5(P\$*.(3@.(/%#(7%/6(C@/"@++ ,0(@.(#\$6(J5h5;?(N6&/6+(9%/H*I"&@#*%/(H*+6(9%/#@*/.(/6@&+, (K0???(+*/6.(%H(% :#*%/.5(B@#\$6&0(@/(BSW(:@9N@I6(H%&(\$6(J5h5;?(N6&/6+(86&.*%/(3@.(7%3/ +@%767(H&%C(^LB6:%5%&I0(@/7(\$6(a9%/H*Ib(H*+6(3@.(6M#&@9#67(H&%C(*#5(B"/ */I(IC@N6(%+79%/H*I1(3*#\$(#\$*.(9%/H*I"&@#*%/(H*+6(&6#"&/67(/%(% "#: "#0(9%/H*&C*/I(\$@#(@++(% :#*%/.(H%&(\$6(J5h5;?(N6&/6+(36&6(76H*/675(

P\$6(/%/QABDE(@/7(ABDE(N6&/6+.(/66767(#%(16(6@.*+, (7*HH6&6/#*#675(] /6(%H(\$6(9% :*6.(%H(\$6(N6&/6+.(%"&96(9%76(3@.(9%/H*I"&67(#%(@: :6/7(\$6(.#&*/I(aQ/%/QN&.*b(#%(*#.(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|;Z(
!

86&.%/5(P\$6(%#\$6&(3@.(9%/H*I"&67(#%(@::6/7(#\$6(.#&*/I(aQN&.*5b(P\$*.(@++ 3 67(H%&(X"*9N(
*76/#*H*9@#%*/(%H(#\$6(N6&/6+(*/(".6(1,(&"//*/I(1"/@C6(Q&I5(
ABDE(3@.(6/@1+67(*/(#\$6(+##6&(N6&/6+(3*\$(#\$6(H%++ 3*/I(9%/H*I"&@#%*/(9\$@/I6.'((

```
CONFIG_BPF_LSM=y
CONFIG_LSM="yama,loadpin,safesetid,integrity,selinux,smack,tomoyo,apparmor,bpf"
CONFIG_DEBUG_INFO_BTf=y
```

(
"\$#\$%&'!(D)!8#, %/!B'&, 'C!J)Q)(V! ? 0, 1#\$%&. -#0, @!-0!F, .2! ' !B< *0(
P\$6(H*#. #(+*/6(6/@1+67(ABDE(*/.#&"C6/#@#%*/5(P\$6(.69%/7(+*/6(:&%8*767(@(+*.#(%H(
LDW.(#%(*/*#*@+*d0(3*\$(ABDE(&6:&6.6/#67(1, (#\$6(3 %&7(a1:Hb(@#(#\$6(6/7(%H(#\$6(.#&*/I5(P\$6(
6/#&*6.(*/(#\$6(+*.#(16.*76.(a1:Hb(3 6&6(* /9+"767(*/(#\$6(76H@"+#(9%/H*I"&@#%*/5(P\$6(#\$*7(+*/6(
6/."&67(#\$@#(#\$6(N6&/6+(3@.(9% C:*+67(3*\$() SU(P, :6(U%&C@#(F) PUG(. , C1%+.5(W@/ , () SU(
#% %+.(/% 3(76:6/7(% /(* /9+"7*/I() PU(. , C1%+.(*/(#\$6(N6&/6+ \(\$6(. , C1%+.(\$6+:(\$6(* /QN6&/6+(
) SU(k 6&*H*6&(:6&H%&C(C6C%&, (@996.. (@H6#, (9\$69N.(%/(\$6(:&% I&@C(16H%&6(*#(*.(+@%7675(
P\$6(:@\$%+6(1*/@&, 0(:@&#(%H(#\$6(a73 @&86.b(:@9N@I60(@+. %(/66767(#%(16(*/.# @++67(#%(1"*+7(#\$6(
L*/"M(N6&/6+(3*\$() PU(. , C1%+.5(
P\$6(.6&86&.(3 6&6(+*N63*.6(9%/H*I"&67(#%(16@.(.*C*+@&@.(:%..*1+6(#%(6@9\$(%#\$6&5(
^*I\$#(9% C:"#6(/%76.(H%&C(@/(RST(9+".#6&(3 6&6(&6.6&867(H%&(#6.#*/I5(A6&/6+ (.6+69#%*/(3 @.(
\$@/7+67(3*\$(S j ^ (1%#5(^@9\$ (9% C:"#6(/%76(C%"/#67(#\$6(.@C6(&6@7Q%/+, (&%#(H*+6..#6C(
H&%C(@96/#&@+(_UD(.6&86&5((

B"8"\$ (4FG&04:)6.\$H11@/I\$- /0)C1\$

!(1@.\$(.9&*:#(*C"+@#67(#\$6(@9#*8*#, (\$@#(#\$6() TT(.9&*:#.(3 6&6(3 &*##6/(#%(76#69#(
@/7(C*#*I@#65(^86&,(%/6Q#%QH*H#66/ (.69%/7.0(#\$6(.9&*:#(&@/7% C+, (:6&H%&C67(%/6(%H(#\$6(
H%++% 3*/I(@9#%*/.'(
•! T&6@#67(@(/63(%#\$6&Q3 &*#@1+6(H*+6(
•! !7767(%#\$6&Q3 &*#@1+6(:6&C*..%*/.(#%(@/(6M*.*#/I(H*+6(
•! !7767(#\$6(DeE [(1*#(%(@/(6M*.*#/I(H*+6(
•! B@/(@DeE [(6M69"#@1+6(H*+6(
•! !##6C:#67(#%(%:6/(@/(DDR(:&%M,(9%/ /69#%*/(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(|>?(
!

!

- ! !##6C:#67(##(9%/ /69#(##(@&6C%#6(76.#*/@#*%/(%86&(PTS(
- ! !##6C:#67(##(9%/ /69#(##(@&6C%#6(76.#*/@#*%/(%86&(e [S(
- ! !##6C:#67(##(6&C*/@#6(#\$6(ABDE(.9&*:#.(F@.(&%%#G(

P\$*.(.9&*:#(+%II67(@++(@9#*%/.(#@N6/0(3\$*9\$C@++367(H%&(9% C:@&*.%/(16#366/(#\$6(+%I.(
%H(#\$6(@##@9N(.9&*:#(@/7(#\$6(+%I.(%H(#\$6(76#69#*%/(.9&*:#.5(P\$6(.9&*:#(*./9+"767(*/(
!::6/7*M()5(

B"B"\$ %.* /JA@017\$

R*I\$Q:6&H%&C@/96(9% C:"#*/I(@: :+*9@#*%/(.8@&,(*CC6/.6+,(* /(\$%3(\$6,(6M6&9*.6(@
.,. #6C5(P\$6,(9@/(9@" .6(:6&H%&C@/96(1##+6/69N.(*/(:&%96..*/I0(C6C%&,(%:6&@#*%/.0(
H*+6.,. #6C(%:6&@#*%/.0(/6#3%&N(9%CC"/*9@#*%/.0(@/7(C%&65(

U%&(\$*%.(6@.%/0(#\$&66(16/9\$C@&N.(36&6(9\$%.6/(H%&(\$*%.(6.6@&9\$'(M\$:+(H%&(

9% C:"#@#*%/@+(16/9\$C@&N*/I0(@T(:&%I&@C(/@C67(C7.#&6..(H%&[E](16/9\$C@&N*/I0(@/7(
#9:N@+*(H%&(/6#3%&N(16/9\$C@&N*/I5(P\$6.6(16/9\$C@&N.(@&6(76.9&*167(16+%35(

!"!#" \$; 9%- 16&6*97&+\$< , 7' 5%&.8=\$35 -+\$

P\$6(R*I\$Q\$S6&H%&C@/96(L*/:@9N()6/9\$C@&N0(%&(M\$:+0(C6@."&6.(#\$6(9% C:"#@#*%/@+(
:6&H%&C@/96(%H(\$6(+@&I6.#(.":6&9% C:"#6&.(*/(\$6(3%&+75(E#(.%+86.(@(.6&*6.(%H(+*/6@&(

@+I61&@ (6X"@#*%/.(##(C6@."&6(\$6(C@M*C"C(aH+:.0b(%&(H+%@#*/IQ:%*/#(%:6&@#*%/.(:6&(

.69%/70(#\$@#(9+" .6&(*.(9@:@1+(%H5(E#(9@/(C6@."&6(\$6(H+:.(%H(@(.*/I+6(9% C:"#6(/%76(%&(

C"+#*:+6(9% C:"#6(/%76.(3%&N*/I(* /("/*.%/5(

P\$6(M\$:+(16/9\$C@&N(3@.(&"/(%/(\$6(6*I#(#6.#(/%76.(*/7*8*7"@++ ,5(U%&(6@9\$(/%760(
#(&@/(\$\$&#,(#*C6.(%/(\$6(/%/QABDE(N6&/6+0(#*\$&#,(#*C6.(%/(\$6(ABDE(N6&/6+(3*#\$%"#(\$6(
)TT(.9&*:#.(+@%7670(@/7(#*\$&#,(#*C6.(3*#\$(@++(H*86())TT(.9&*:#.(+@%7675(

!"!"0"\$>+ , /?/6 , %\$< , 7' 5%&.8=\$%2/6. , //\$

P\$6(C7.#&6..(16/9\$C@&N(*.(@(&""7*C6/#@&,(T(:&%I&@C(3*##6/(1,(\$*%.(@"#\$%&5(E#(
9&6@#67(@/(63(H*+60(3&%#6(\$6(.#&*/I(aC7.#&6..b(##(*#0(@/7(76+6#67(\$6(H*+6*/(@(#*I\$#(+%#:5(
- \$6/(@++(+%#:.(9% C:+6#670(*#(:&*/#67(\$6(#%#@+6+@:.67(#*C6*/(.69%/7.5(P\$6(:"&:%.6(%H(
#\$*%(16/9\$C@&N(3@.(%#(76#6&C*/6(\$%3(C@92H*+6:6&C.(16\$@867("/76&(6M#&6C6(+@%75(P\$6(
.%"&96(9%76(%H(\$6(:&%I&@C(9@/(16(H%" /7*/(!::6/7*M(T5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE|>;(!

!

^@9\$(C7.#&6..(16/9\$C@&N(3@.(9%/H*I"&67(#%(9% C:+6#6*/(;?(.69%/7.(#@#%:#*C@+(:6&H%&C@/965(!/,(%86&\$6@7(3%"7(9@".6(#.(9% C:+6#*%/(#%(6M9667(;?(.69%/7.5(U%&(6M@C:+60(3\$6/(9&6@#*/I(;??0????*/%76.0(#\$6(.#&6..6&(+%%:(3@.(&@#6(+*C*#67(#%(;?0????+%%:.(:6&(.69%/70(3\$*9\$(@#(*#.H@.#6.#(3%"7(9% C:+6#6*/(;?(.69%/7.5(!/,(.+%37%3/(16,%/7(#\$6(&@#6(+*C*#(3%"7&6."+##*/#\$6(16/9\$C@&N(#@N*/I+%/I6&(#\$@/(;?(.69%/7.(#%(9% C:+6#65(^@9\$(9%/H*I"&@#*%/(3@.(&"/(#\$*&#,(#*C6.(%/6@9\$(/%76(3*#\$(/%())TT(.9&*:#.(&"//*/I0(@/7(#\$6(&6."#.(36&6(6@86&@I675(P\$6.6(#6.#.(36&6&6:6@#67(3*#\$(C@92H*+6:6&C.(&"//*/I(@/7(#\$6/(&6:6@#67(%/6(C%&6(#*C6(3*#\$(#\$6("C@.N(%H(#\$6(C7.#&6..(:`..(6#(##(???0(3\$*9\$(&6."#67*/(\$6(-]PR(1*(16*/I(.6#(%/(\$6*/%76.5(U*+6(@/7(7*&69%#&,(9@9\$6.(36&6(7&%::67(16H%&6(6@9\$(&"/(#%(C*/*C*d6(#\$6(6HH69#(%H(9@9\$*/I(16#366/(&"/.5(

!"!4"\$ @,6A9.8\$<,7'5%&.8=\$6' -8&+*\$

P\$6(#9:N@+(16/9\$C@&N(9@/(6.#@1+*.\$(@/7(#6@&(7%3/(\$%"".@/7.(@/7(686/(C*++%/.(%H(PTS(9%/ /69#*%/.(*/(@(.%&#(:6&*%7(%H(#*C65(E#(*."67(#%(.#&6..0#6.#(@: :+*9@#*%/.(@/7(/6#3%&N.5(U%&(\$*.(&6.6@&9\$0(*#(\$6+:67(*76/*#H,(\$6(:6&H%&C@/96(9%#(%H(@##@9\$*/I(:&%I&@C.(#%(\$6(.%9N6#29%/ /69#(LDW(\$%%N5(

P\$*.(16/9\$C@&N("67(%/6(9% C:"#6(/%76(@.(@9+*6/#5(E#("67(":(#%(.686/(/%#\$6&(9% C:"#6.(/%76.(H%&(76.#*/@#*%/.5(P\$6(9% C:"#6(/%76.(36&6(@++(#"/67(#%(@++%3(":(#%(JJ0???)(PTS(9%/ /69#*%/.(:6&(:66&5(P\$6.6(#"/*/I.(9@/(16(H%"7(*/(!: :6/7*M([5((

P\$6(9+*6/#(@##6C:#67(;0J??(PTS(9%/ /69#*%/.(:6&(.69%/7(:6&(76.#*/@#*%/(0.9@+*/I(":(#%(;?0J??(PTS(9%/ /69#*%/.(:6&(.69%/7(3\$6/(@++(.686/(76.#*/@#*%/.(36&6*/("65(^@9\$(&"/(3@.(I*86/(@(\$*&#,Q.69%/7(#*C6(+*C*#0(@/7(#\$6/("C16&(%H("996..H"+(9%/ /69#*%/.(3@.(&69%&767(1,(\$6(/%76.(@9#*/I(@.(76.#*/@#*%/.5(P\$6(76.#*/@#*%/(/%76.(&@/(1.9@#I(#%(*#6/(H%&(@/7(&69%&7(PTS(9%/ /69#*%/.5(P\$6.6(#6.#.(36&6(&"/(3*#\$(#(C@92.N9%/ /69#*%/.(+%@767(@/7(3*#\$(#+%@767(#%(9% C:@&6(:6&H%&C@/965(

C#!4 / ; *1&;!

P\$6(16/9\$C@&N(&6."#.(.\$%367(\$@#(\$6())TT(.9&*:#.(:6&H%&C67(86&,(H@8%&@1+,(" /76&*/#6/.*86(1"#(#6@+*.*#9(3%&N+%@7.5(R%3686&0(3\$6/(C7.#&6..(@/7(#9:N@+*(:". \$67(.,.#6C.(#%(86&,(6M#&6C6(+686+.0(6/%"I\$(#%(76I&@76(I6/6&@+(.,.#6C(:6&H%&C@/960(\$6/(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>>(!

!
&"//*/I(#\$6() TT(.9&*:#.(3%&.6/67(:6&H%&C@/965(P\$%.6(6M#&6C6(3%&N+%@7.(@+.%(
%86&+%@767(#\$6(a:6&H(&*/I(1"HH6&0b(3*\$9\$(3@.(#\$6(1"HH6&(" .67(1,() SU(%(.#&6@C(\$*I\$(
8%+"C6.(%H(N6&/6+(686/#.(#%(" .6&Q.:@965(P\$*. (7*7(/%#(*C:676(#\$6() TT(.9&*:#.(*/(
:&686/**/I(@##@9N.0(1"#(*#(7*7(@HH69#(#\$6*&(@1*+*#,(#%(+%I(#\$6C5((

K"#"\$ L.1./1)4*\$>.7+617\$

["&*/I(#\$6(M\$:+(16/9\$C@&N.0(#\$6(@786&.@&,(6C"+@#*%/(.9&*:#(@/7(@++(#\$6() TT(
.9&*:#.(&@/(@/7(+%II67(#\$6*&(@9#*8*#*6.5(P\$6.6(+%I.(36&6(@II&6I@67(#%(76#6&C*/6(3\$6#6&(
#\$6(@9#*%/.(1,(#\$6(@786&.@&*@+(.9&*:#(36&6(. "996..H"++,(76#69#67(@/7(C*#*I@#675((

! ++(C@+*9*%".(H*+6(@9#*8*#*6.0(* /9+"7*/I(9&6@#*/I(3%&+7Q3&*#@1+6(H*+6.(@/7(@77*/I(
-] PR(%&(DeE [(1*#.0(36&6(+%II67(@.(a76/*67b(6M96:#(H%&(%/6(%H(#\$6(>0Z`=(a!77(-] PR(
1*#b(@9#*%/.5(! ++(@##6C:#.(#%(&"/(DeE [(6M69"#@1+6.(36&6(76/*67(@/7(+%II675(! ++(@##6C:#.(
#%(%:6/(DDR(:&%M*6.(36&6(+%II67(@.(a76/*67b(6M96:#(H%&(#3%(%H(#\$6(>0Z=c(ES8=(@##6C:#.5(
! ++("/@#"#\$%&*d67(.%9N6#(9%//69#*%/(@##6C:#.(@/7(@++(@##6C:#.(#%(N*++(#\$6() TT(.9&*:#.(36&6(
76/*67(@/7(+%II675(

E#(3@.(7*HH*9"+#(#%(76#6&C*/6(#\$6(9@" .6(%H(#\$6(#\$&66(C*..*/I(+%I.(7"6(#%(@(
.\$%	%C*/I(%H(#\$6(@##@9N(.9&*:#(*#.6+H5(P\$6(@##@9N(.9&*:#(+%II67(3\$@#(@9#*%/.(*#(3%" +7(
#@N60(1"#(*#(7*7(/%#(&69%&7(3\$6#6&(#\$6(@##6C:#67(@9#*%/(3@.(6M69"#67(%&(/%#5(E#(3@.(
:%. .*1+6(#\$@#(@H63(C@+*9*%".(@9#*%/.(H@*+67(H&%C(&6I"+@&(. ,. #6C(6&&%&.5(P\$*. (3%" +7(\$@86(
@9#67(@.(@(. \$%&#Q9*&9"*#(:&%&(#%(\$6(LDW(\$%N(16*/I(#&*II6&67(@/7(#\$6() TT(.9&*:#(9%C*/I(
*/#%(:+@,5(

P\$6(&6."+.#.(@&6(. "CC@&*d67(16+%3(*/(U*I"&6(;=5(

(
(
(
(
(
(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(|>c(

!

W@+*9*%".(!9#*%/(T%" / #(ABDE(D9&*:#([6/ ,([6/ ,(P , : 6.(P , : 6(T%" / #((
T&6@#6(-] PR(>ZZK(((9&6@#6(>ZZK(
! 77(-] PR(>Z`=(C@92H*+6:6&C.(hZ?K(9\$C%7(F?`?>G(>Z`J(
! 77(DeE [(>Z= `(((9\$C%7(F=`??G(>Z= `(
B"/(DeE [(>ZhZ(C@92."*76M69(>ZhZ(6M."*7(>ZhZ(
DDR(S&%M,(>Z=J(C@92..\$+.#6/6&.(Jhhh(ES8=(>Z=c(
((((ES8 `(>Z=J(
D%9N6#(T% // 69#(>Z;h(C@92.N9% // 69#(>Z;h(ES8=(>Z;h(
A*+() TT(FH*+6:6&C.G(Jh `(N*+@.N.(FH*+6G(; ;K `(H*+6:6&C.(%/+, (Jh `(
A*+() TT(F."*76M69G(`?>(N*+@.N.(F."*7G(; ;Z>(."*76M69(%/+, (`?>(
A*+() TT(F..\$mG(`??(N*+@.N.(F..\$mG(; ;Z?(..\$+.#6/6&.(%/+, (`??(
A*+() TT(F.N9% // 69#G(`>;(N*+@.N.(F.N9mG(; >;;(.N9% // 69#(%/+, (`>;(
A*+() TT(FN*+@.N.G(JZ?(((((

(

"#\$%&'!(E)!W.2C'!0!9.C#4#0%@!:4-#0,!?0%,-@!.,>!9:?!X',#.C! ?0%,-@!(

- \$*+6(\$6(M\$:+(76#69#*%/(&6."#+.(3 6&6(86&,(H@8%&@1+60(\$6(#9:N@+*(@/7(C7.#&6..(

16/9\$C@&N.(76C%/.#&@#67(\$@#(@/(6M96..*86(@C%"/#(%H(W!T(686/#.(9%"+7(&6."#+*(/(

7&%::67(+%I.5(P\$6.6(76#@*+.(3*+(16(7*.9"..67(@.(:@&#(%H(\$6(:6&H%&C@/96(&6."#+.5(

K"!\$ &.0:40A@* / .\$> .7+617\$

P\$&66(%%+.(C6@."&67(\$6(:6&H%&C@/96(*C:@9#(%H(ABDE'(M\$:+0(C7.#&6..0(@/7(

#9:N@+*5(- \$*+6(M\$:+(3 @.(9%/H*I"&67(#%(" .6(@(+@&I6(1"#(&6@.%/@1+6(:%&#*%/(%H(6@9\$(.,.#6CV.(

9%C:"#@#*%/@+(&6.%"&96.0(C7.#&6..(@/7(#9:N@+*(.9@+67(E] (@/7(/6#3 %&N(+%@7.(:@.#(

&6@.%/@1+6(.,.#6C(9@:@1*+*#6.5(D#&6..(#6.#/IE] (@/7(/6#3 %&N(&6.%"&96.(*/(\$*.(C@//6&(

&686@+67(\$6(16\$@8*%&(%H(ABDE(%/(. ,.#6C.("HH6&*/I(H&%C(6M#&6C6(+%@7.5((

P\$*.(.69#*%/(:&6.6/#.(\$6(16/9\$C@&N(&6."#+.(@.(9\$@&#.\(\$6(/ "C6&*9(#@1+6.(".67(#%(

I6/6&@#6(\$6.6(9\$@&#.(9@/(16(H%"/7(*/(! : :6/7*M(^5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>=(
!

!

(

"#\$%&'!(J)!?;.&-!0!\$;/;3T!<'@%L-@!

ABDE(\$@7(@(+6..(#\$@/(; n(9% C:"#@#%/@+(*C:@9#(%/(M\$:+(16/9\$C@&N.(%/(\$6(
9% C:"#6(/%76.5(P\$6(3%&. #9@.6(3@.(_%76(`0(3\$*9\$(6M\$*1*#67(@(?5;= n(:6&H%&C@/96(+%..(
3\$6/(".* /I(@ABDEQ6/@1+67(N6&/6+(3*\$(@+() TT(.9&*:#.(+%@7675(] 77+,0(_%76(>(. \$% 3 67(@(
?5J; n(I@*/(*/(:6&H%&C@/96(3*\$() TT(.9&*:#.(+%@7670(1"#(#\$*.(3%" +7(/%#(16(6M: +@*/67(1,(
ABDE5(E#(3@.(+*N6+, (7"6(#%(%#\$6&(H@9#%&.(*/(\$6(#6.#(6/8*&%/C6/#0(. "9\$(@.(/6#3%&N(
9%/#6/#*%/(H&%C("/&6+@#67(9% C:"#6(/%76.(%&(. ,.#6C(0*##6&5(P\$6(&6.#(%H(\$6(/%76.(. \$% 3 67(@(
:6&H%&C@/96(9\$@/I6(%H(?5?J n(%&(+6..(16#366/(\$6(/%/QABDE(N6&/6+(@/7(\$6(ABDE(N6&/6+(
3*\$() TT(.9&*:#.(&"/ */I5(

W**I@#*/I(!##9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>J(!

!

(

(

"#\$%&'!(K)!?;.&-!0!\$A>@-&'@@T!<'@%C-@

P\$6(C7.#&6..(16/9\$C@&N(&686@+67(#3%(*.."6.(3\$6/("/76&(6M#&6C6(H*+6.,.#6C(+%@75(U*&.#0(*H(@9%C:"#6(/%76(3@.(.#&6..67(3*\$(C%&6(H*+6(9&6@#*%/(%:6&@#*%/(.#\$@/(*(9%"7(\$@/7+60(\$6/(&"//*I())TT(.9&*:#.(#\$@#(C%/*%&67(H*+6(9&6@#*%/(3%"7(C@N6(\$6(:&%1+6C(3%&.65(D69%/70(3\$6/(686/#.(36&6(I6/6&@#67(1,(\$6(N6&/6+Q.:@96(:&%I&@C(#%%(X"*9N+,0(\$6(:6&H(&*/I(1"HH6&(3%"7(%86&3*#6(\$6(%+76.#(686/#(7@#(16H%&6("6&Q.:@96(.9&*:#.(+%II67(*#5(P\$*(3@.(*/7*9@#67(1,(C6..@I6.(H&%C(\$6())TT(.9&*:#.(#@#*/I0(aS%..*1+,(+%.#(_(.@C:+6.0b(3*\$(C@/I*/I(H&%C(;(#%(%86&@C*+*%/0(76:6/7*/I(%/(\$6(+%@7(\$6@#(C7.#&6..(:+@967(%/(\$6(.9&*:#5(

(- \$6/(\$@/7+*/I(;?0???(*/%76(9&6@#*%/(686/#.(6&(.69%/70(\$6(C@92H*+6:6&C.(.9&*:#(7*7(/%#(9@".6(:6&H%&C@/96(+%..(*.."6.0(1"#*(7*7(7&%:(+%I.(7"6(#%(\$6(%86&3\$6+C67(&*/I(1"HH6&5(

((

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>`(
!

!

(

"#\$%&'!(P)!?;.&-!0!\$-43I.0#T!<'@%0-@(
!

P\$6(#9:N@+*(16/9\$C@&N(.#&6..67(#\$6(.,.#6C(16,%/7(*#.(@1*+*#,(#%(C@*/#@*/(*#.(
9%/ /69#*%/(&@#6(3\$6/(.6#(#%(Z)???PTS(9%/ /69#*%/.(:6&(.69%/75(P\$*.(:6&H%&C@/96(
76I&@7@#*%/(169@C6(3%&.6(@#(;?0J??(PTS(9%/ /69#*%/.(:6&(.69%/75(P\$6(
C@92.N9%/ /69#*%/.(.9&*:#(16I@/(#%(+% .6(+I.(H&%C(#\$6(:6&H2&* /I21"HH6&(@#(\$\$*.(:%*/#5(E/(
1%#\$9@.6.0(@##@9\$*/I(C@92.N9%/ /69#*%/.(9@" .67(#\$6(.,.#6C(#%(:6&H%&C(.+*I\$#+,(3%&.65(
!

D#!B(%+1* ;, (% ;!<%)!E* &* ' /! F ('G!
!

B"//*/I() TT(.9&*:#.(3*\$(ABDE(7*7(/%#(9@" .6(:6&H%&C@/96(+%..(" /+6..(#\$6(.,.#6C(
3@.(@+&6@7,(. "HH6&* /I(H&%C(76I&@767(:6&H%&C@/965(E#(7*7(/%#(*C:@9#(M\$:+(16/9\$C@&N.5(E#(
%/+,(*C:@9#67(C7.#&6..(@/7(#9:N@+*(16/9\$C@&N.(@H#6&(6M#&6C6(+%@7.(36&6(@+&6@7,(9@" .*/I(
I6/6&@+(.,.#6C(:6&H%&C@/96(:&%1+6C.5(P\$6&6H%&60(9% C:@/*6.(@/7(%&I@/*d@#*%/.(.\$%" +7(
9%/##/"6(* /86.#*I@#*/I(ABDE(H%&(@7%:#*%/(*/(RST(@/7(* /H%&C@#*%/(.69"&*# ,5(
!

P\$6() TT(.9&*:#.(@::6@&67(#%(.#*+*(C*#*I@#6(@##@9N.(686/("/76&(6M#&6C6(+%@70(1"#(
#\$6,(7*7(/%#(I"@&@/#66(d6&%(+%..(%H(+I.5(- \$6/(\$6(H*+6.,.#6C(686/#&@#6(@::&%@9\$67(\$6(
%&76&(%H(;? ?0??? (H*+6(9&6@#*%/.(:6&(.69%/70(\$6(C@92H*+6:6&C.(.9&*:#(7&%::67(C*+*%/.(%H(
!

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>K(!

! * /9% C* /I(+% I.5(P\$*.(./%#(@(. \$%	% C* /I(%H(ABDE0(1"#(&@#6&(*.(\$6(6M:69#67(9% / .6X"6/96(%H(%86&+%@7* /I(@&* /I(1"HH6&5(E#(*.(:%..*1+6(#%(* /9&6@.6(\$6(:6&H(&* /I(1"HH6&V.(.*d60(1"#(\$6(76H@"#(*.(@+&6@7,(`=(:@I6.(:6&(TS e(F [&@ ,#% /G5(! / ,(+%@7(#\$@#(%86&3\$6+C.(#6(:6&H(&* /I(1"HH6&(\$@.(@+&6@7,(:". \$67(\$6(. ,. #6C(36+(16,% /7(&6@.% /@1+6(+*C*#.5((

ABDE(3*+(169% C6(C"9\$(C%&6(@: :&%@9\$@1+6(% /96(1:H#&@96(.": :%&#.(*5(P\$*.(#%#+(:&%8*76.(@ /(! - A0+*N6(. , /#M(#\$@#(*.(C"9\$(C%&6(* /#"**86(#%(. ,. #6C.(@7C* /*. #&@#%&.(@ /7(* /H%&C@#*% /(.69"%*#,(:&@9#*#*% /6&.(#\$@ /(\$6(9% C : +6M() TT(.9&* :#. (3 &*##6/(H%&(#\$*.(&6.6@&9\$5(

P\$%.6(* /#6&6.#67(* / (ABDE9@ / (/ %3 (6M:6&*C6/#(3*\$(*#(" . * /I(#6(.#%9N(N6&/6+(%H(@ (C@0%&(L* / "M(7* .#&*1" #*% /5(T@ / % / *9@+(&6+6@.67(\$6(>?; ?(86&.*% /(%H(e 1" /#" (%) /(>>(>] 9#%16& (>?>?0(@ /7(*#(& " / .(% /(\$6(J5h(L* / "M(N6&/6+5(e .6&.(9@ / (6/@1+6(ABDE(1,(. :69%H,* /I(a1:Hb(* / (#6(a+.Cb(N6&/6+(:@&@C6#6&(F65I50(a+.Co+o9N7%3 /0 ,@C@0* /#6I&*# ,0@: :@&C%&01:HbG5((

P\$*.(@"#\$%&(" .67(@ (N6&/6+(9% /H*I"@&*% / (1@.6+* /6(#\$@#(\$@7(C@ / , (LDW.(* / *#*@+*d670(3\$*9\$(C@ , (\$@86(7&%3 /67(% "#(\$6(#&"6(:6&H%&C@/96(*C : @9#(%H(6/@1+* /I(ABDE5(U"#"&(&6.6@&9\$(9@ / (C6@." &6(\$6(:6&H%&C@/96(%H(. ,. #6C.(3*\$(6*#\$6&(/%(LDW.(* / *#*@+*d67(%&(/+ , (ABDE(* / *#*@+*d675(

P\$6(.9&* :#. (3 &*##6/(H%&(#\$*.(&6.6@&9\$(" .67(% /+ ,(. *M(LDW(\$%N.0(1" #(\$6&6(@&6(>cc(LDW(\$%N.(@8@*+@1+6(* /(\$6(J5h5; ?(L* / "M(N6&/6+5(E#(3%" +7(16(8@+@"@1+6(H%&(#\$%.6(3*\$(N6&/6+(7686+% : C6/#(@ /7(* /H%&C@#*% /(.69"%*#,(6M:6&*6/96(#%(3 &*#6(77*#*% /@+()) TT(.9&* :#. (#6@#(+686&@I6(#6.6(LDW(\$%N.(* / * /#6&6.#* /I(/63(3@ ,.5((

] /96(ABDE(*.(I6/6&@+ , (@8@*+@1+60(RST(6/8&% / C6/#.(9@ / (: %6 /#*@+ , (9%" : +6(*#(3*\$(#\$6*(&(.9\$67"+6&.(#%(@ " /9\$9".#%C(W ! T(:%+*9*6.(:6&(9% C : "#6(/%760(1@.67(% /(\$6(".6&.V(0%1.(7*.: @9\$67(#%(\$% .6(/%76.5(P\$*.(3%" +7(&6."#(* /(. :69*+@(.69"%*#,(C6@."&6.(#\$@#(H%+ %3 (" .6&.(#% (3\$*9\$686&(/%76.(#\$6*(&6.6@&9\$*.(&" / * /I(% /5(

P\$6(" +*C@#6(16/6H*#(%H(ABDE(*.(\$6(H&667% C(*#(I*86.(. ,. #6C.(@7C* /*. #&@#%&.(#% (1"*+7(9&6@#86(/63(W ! T(:%+*9*6.5(P\$%.6(3\$%(3 %&N(% / (L* / "M(. ,. #6C.(3*\$(&696/#(N6&/6+.(@&6(6/9%"&@I67(#%(& , (ABDE0(16(9&6@#86(* /(*#.(".@I60(@ /7(. \$@&6(\$6*(&* / %8@#*% /(.3*\$(#\$6(9%CC" / *# ,5(

(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>h(
!
! "#\$"%&" '(
)@&N+6,0(Y5(F;ZZ=G5([*.9&6#*%/@&,(!996..(T%/##%+5(6789%85)I'##%:;<"'I#0',*%=>>?@5(
B6#&*6867(>`(D6:#6C16&(>?>?(H&%C((
\$##: '<H#:5I/%C65%&I<C*%&%&&<@&9\$*86<H#:5."/6#5.6<:"1<.69"&*#,<7%9.</*#:"1.<h??Q
K<C@*/5\$#C+(
)6@##*60(D5(F>?;KG5(!1%"#(!::!&C%&5(A55A.2,.%8)I;.'0\$%:. ,B)I0% C'D'5(B6#&*6867(>`(
D6:#6C16&(>?>?(H&%C(\$##:.'<I*#+@159% C<@::@&C%&<@::@&C%&<Q<3*N*.<!1%"#(
)%&NC@//0([5(F>?>?G5(W6&I6(1&@/9\$(p1:HQ+.CV(qT% C:"#6&(D%H#3 @&6r5(E).*)"F, .3%3'0%
.)5, ('0, . ')(F(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<I*#5N6&/6+5%&I<:"1<.9C<+*/"M<N6&/6+<I*#<#%&8@+7.<+*/"M5I*#<9%CC*#<i*7o`=;9
7K1?'9Z;;9JZcJ9c=H>=hJ?6@;h`Z?'=ZZ;K(
T%%N0(A5(F>?;?G5(.69"&*#,'(g@C@(LDW(qT% C:"#6&(D%H#3 @&6r5(GC65(B6#&*6867(>`(
D6:#6C16&(>?>?(H&%C(\$##:.'<<+3/5/6#<!&#*9+6.<cZc?;><(
T%%N0(A5(F>?;KG5(DC@9N5(9+)%G'*;4%D).*)"%;().H(%##*/%#/2'*'(0.#0,.H(%3;'/)F(B6#&*6867(
>`(D6:#6C16&(>?>?(H&%C(\$##:.'<<3335N6&/6+5%&I<7%9<\$#C+<8=5;J<@7C*/Q
I"*76<LDW<DC@9N5\$#C+(
T%&16#0(Y5(F>?;Z0([9#%16&G5())SU(@#(U@961%%N(F@/7(16,%/7G5(GC6F(B6#&*6867(>`(
D6:#6C16&(>?>?(H&%C(\$##:.'<<+3/5/6#<!&#*9+6.<h?;hK;<(
T%&16#0(Y5(F>?;Z0([696C16&G5(ABDE(s(#\$6(%#\$6&())SU(.69"&*#,(C%7"+65(GC6F(B6#&*6867(>`(
D6:#6C16&(>?>?(H&%C(\$##:.'<<+3/5/6#<!&#*9+6.<h?h?>=h<(
T%&16#0(Y5(F>?>?0(Y"/6G5(P\$6(J5K(N6&/6+(*.(%"#5(GC6F(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<+3/5/6#<!&#*9+6.<h>;h>Z<(

W**I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(|>Z(
!
[&@, #%/0(W5(F>?;K0(U61&"@&,G5(W@N6(:6&H(&*/I(1"HH6&(. *d6(9%/H*I"&@1+6(qT%C:"#6&(

.%H#3 @&6r5(I '0+; <5(B6#&*6867(>; (] 9#%16&(>?>?(H&% C(

\$##:.'<<I*#\$"159%C<*&8*.%&<199<:"++ZZK(

[&,.7@+60([5(F>?;JG5(R%3(:&%I&@C.(I6#(&"/5(GC6F(B6#&*6867(;K(] 9#%16&(>?>?(H&% C(

\$##:.'<<+3/5/6#< ! &#*9+6.<`c?K>K<(

^7I60(Y5(F>?;JG5(S&%I&6..(*/(.69"&*#,(C%7"+6(.#@9N*/I5(GC6F(B6#&*6867(>`(D6:#6C16&(

>?>?(H&% C(\$##:.'<<+3/5/6#< ! &#*9+6.<`cJKK;<(

f &6II0()50(6#(@+5(F>?;`G5()99(S,\$\$%/([686+%;6&(P"#%&*@+5(I '0+; <5(B6#&*6867(; (] 9#%16&(

>?>?(H&% C(

\$##:.'<<I*#\$"159%C<*&8*.%&<199<1+%1<C@.#6&<7%9.<#"#%&*@+21992:,\$\$%/27686+%;6&5C

7(

f &6II0()5(F>?;h0(D6:#6C16&G5(I6#\$%.# +@#6/9,51#(qT%C:"#6&(.%H#3 @&6r5(I '0+; <F(B6#&*6867(

>`(D6:#6C16&(>?>?(H&% C(

\$##:.'<<I*#\$"159%C<*&8*.%&<1:H#&@96<1+%1<C@.#6&<#%+.<I6#\$%.# +@#6/9,51#(

f &6II0()5(F>?>?0(Y@/"@&,G5(J:K%:).L,.2#*1)%9,, "(M%G'*;4%8\$(0)2%#*/%A55"1#0',*%
N<().-#<""0\$5(e / *#67(D#@#6.'(!77*.%/Q - 6.+6,5(

f &6II0()50(6#(@+5(F>?>?0(!"I".#G5(199(B6H6&6/96(f"*765(I '0+; <5(B6#&*6867(>`(D6:#6C16&(

>?>?(H&% C(\$##:.'<<I*#\$"159%C<*&8*.%&<199<1+%1<C@.#6&<7%9.<&6H6&6/962I"*765C7(

f &6II0()50(6#(@+5(F>?>?0(D6:#6C16&G5(1:H#&@96(B6H6&6/96(f"*765(I '0O; <F(B6#&*6867(>`(

D6:#6C16&(>?>?(H&% C(

\$##:.'<<I*#\$"159%C<*&8*.%&<1:H#&@96<1+%1<C@.#6&<7%9.<&6H6&6/962I"*765C7(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$ (ABDE(| c?(!

!

f &6II0() 50(t (W@6.#&6##*0(! 5(F>?;K0(U61&"&#,G5(D69"&*#,(W%/ *%&* /I(3*#\$(6) SU5(E/(

J8'/(8K%P>Q@0(D@/(U&@/9*.9%0(T!5(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(

\$##:.'<<3 3 35,%""1659%C<3@#9\$ i8o==/k`W0;;"3(

A6&*.N0(W5(F>?;?G5(9+)%G'*;4%:. ,3.#2 2 '*3%7*0).L#1)M%A%G'*;4%#*/%R67S%(\$ (0) 2%

5.,3.#2 2 '*3%+*#/<, ,DF%D@/(U&@/9*.9%'(_%(D#@&9\$(S&6..5(

L@&@16+0(W5(F>?>?G5(P\$6(S6&H%&C@/96(T%.(#%(D^L*/"M(%/(U67%&@ (c;5(:+,.,* '45(

B6#&*6867(;=(_%86C16&(>?>?(H&%C(

\$##:.'<<3 3 35:\$%&%/*M59%C<8&5:\$: i8*63 o>hKZh(

_@#*% /@+(E/.#*#"#6(%H(D#@/7@&7.(@/7(P69\$/%+%I,5(F>?;`G5(!/(!9#*%/(S+@/(H%&(R*I\$(

S6&H%&C@/96(T%C:"#*/I(D69"&*#,0(- %&N*/I([&@H#5(f @*#\$6&.1"&I0(W[5(B6#&*6867(

>`(D6:#6C16&(>?>?(H&%C(

\$##:.'<<3 3 35/*.#5I%8<.,.#6C<H*+6.<7%9"C6/#.<?>;h<?c<;J<3%&N*/I27&@H#2@9#*%/:+

@/\$:95:7H(

] +.@0(Y5(F>?>?G5(!77(+.C(:&%16(.": :%&#(qT%C:"#6(D%H#3 @&6r5(B6#&*6867(>`(D6:#6C16&(

>?>?(H&%C(\$##:.'<<I*#\$"159%C<*%8*.%&<1:H#&@96<:"++<;c=K(

D*/I\$0(A5(F>?;Z0(D6:#6C16&G5(A6&/6+(B"/*#C6(D69"&*#,(E/.#&"C6/#@#*%/5(GC65(B6#&*6867(

>`(D6:#6C16&(>?>?(H&%C(\$##:.'<<+3/5/6#<!&#*9+6.<KZhZ;h<(

D*/I\$0(A5(F>?;Z0([696C16&G5(+.C2@"7*#26/859(qT%C:"#6&(D%H#3 @&6r5(I'0+;<5(B6#&*6867(;(

]9#%16&(>?>?(H&%C(\$##:.'<<I*#\$"159%C<.* /N@:<+*/"MQ

N&.*<1+1<:@#9\$<8;<6M@C:+6.<.@C:+6.<1:H<+.C2@"7*#26/859(

D*/I\$0(A5(F>?>?0(W@&9\$G5(W!T(@/7(!"7*#(S%+9,(".* /I(6) SU(FABDEG5(GC6F(B6#&*6867(>`(

D6:#6C16&(>?>?(H&%C(\$##:.'<<+3/5/6#<!&#*9+6.<h;Jh>`<(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE(| c;(

!
D*/I\$(A5(F>?>?0(Y"+,G5(ABDE(F)SU(u(LDWG(s(e:7@#6.(@/7(S&%I&6..5E/(G'*;4%8)I;. '0\$%
8;22'0%6,.0+.%A2). 'I#0(k*&#"@+(T%/H6&6/96F(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<%../@>?>?5.9\$6759% C<686/#<9N:L<N&. *Q1:HQ+.CQ":7@#6.Q@/7Q:&%I&6..QN:Q
.* /I\$QI%%I+6(
D*/I\$(A50(6#(@+5(F>?>?0(D6:#6C16&G5(\$@3N(qT% C:"#6&(D%H#3 @&6r5(I '0+; <5(B6#&*6867(;K(
]9#%16&(>?>?(H&%C(\$##:.'<<I*#\$"159% C<I%%I+6*/#6&/.<\$@3N(
DC@++6,0(D50(6#(@+5(F/575G5(L*/"M(D69"&*#,(W%7"+6.'(f6/6&@+(D69"&*#,(R%N.(H%&(L*/"M5(9+)%
G'*;4%E).*)%A.I+'-)(F(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<3335N6&/6+5%&I<7%9<\$#C+<+@#6.#<.69"&*#,<+.C5\$#C+(
DC@++6,0(D50(6#(@+5(F>?>?0(Y"/6G5(L*/"M(D69"&*#,(W%7"+6(U&@C63%&N5E/(N00#T##G'*;4%
8\$25,(' ;20(]##@3@0(]/#@&*%0(T@/@7@5(B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<9*#6.66&M5*.#5:."567"<8*637%9<7%3 /+%@7i7%*o;?5;5;5;;Z5;`? = t &6:o&6:; t #
,:6o:7H(
DC@++6,0(D50(6#(@+5(F>?>?0(W@,G5(EC:+6C6/#*/I(D^L*/"M(@.(@ (L*/"M(D69"&*#,(W%7"+65(
B6#&*6867(>`(D6:#6C16&(>?>?(H&%C(
\$##:.'<<3335/.@5I%8<S%&#@+.<K?<*C@I6.<&6.%"&96.<686&,%/6<7*I*#@+QC67*@Q
96/#6&:<"1+*9@#*%/.<&6.6@&9\$Q:@:6&.<*C:+6C6/#*/IQ.6+/"MQ@.Q+/"MQ.69"&*#,Q
C%7"+6Q&6:%:7H(
D%/I0(g5(F>?>?G5(:&6:@&6(H%&(&6+6@.6(8?5;J5?(qT% C:"#6&(D%H#3 @&6r5(I '0O; <F(B6#&*6867(>`(
D6:#6C16&(>?>?(H&%C(
\$##:.'<<I*#\$"159% C<*%8*.%&<199<9% CC*#<6=;HK@c16J9h;;=6H`@?ZZ?6J?9>H1@16@?6Z
>h6v7*HHQ=J9;K9?@?h?H16>Z6>1h767hZ=?@@;6h(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*\$(ABDE(| c>(
!

! P@N67@0(A5(F>??ZG5(P]W]g](L*/"M(]86&8*635(S&6.6/#67(@#"':4%I,*L%#;0(R%1@�(
!

!"#&@+*5(B6#&*6867(>^(D6:#6C16&(>?>?(H&%C(
!

\$##:.'<%7/5/6#<:&%069#.<#%C%,%<7%9.<+9@>??ZQ#N67@5:7H(
!

WEPB^5(F>?>?0(W@&9\$G5(A6,7/@:5(U79&V%A99W!E5(B6#&*6867(;K(]9#%16&(>?>?(H&%C(
!

\$##:.'<<@##@9N5C*#&65%&I<.%H#3@&6D?>K`<(
!

WEPB^5(F>?>?0(!"I".#G(T-^QKc>'E/9%&&69#(S6&C*..*%/(!..*I/C6/#(H%&(T&*#9@+(
!

B6.%"&965(!,22,*%C)#D*)((%V*;2).#0',*F(B6#&*6867(;K(]9#%16&(>?>?(H&%C(
!

\$##:.'<9365C*#&65%&I<7@#@<76H*/*#*%/.<Kc>5\$#C+(
!

-*+.%/0()5(F>?>?0(Y"/6G5(D69"&*/I(#\$6(D%H#(e/76&16++,(%H(@D":6&9%C:"#6&(3*\$()SU(
!

S&%16.5(8A68%7*(0'0;0)F(B6#&*6867(>^(D6:#6C16&(>?>?(H&%C(
!

\$##:.'<<3335.@/.5%&I<&6@7*/IQ&%%C<3\$*#6:@:6&.<+*/"M<.69"&*/IQ.%H#Q"/76&16++,Q
!

." :6&9%C:"#6&Q1:HQ:&%16.QcZ`cJ(
!

-*+.%/0()5(F>?>?0(]9#%16&G5(199Q+.CQ.9&*:#.(qT%C:"#6&(D%H#3@&6r5(I'0+;<5(B6#&*6867(;K(
!

]9#%16&(>?>?(H&%C(\$##:.'<<I*\$"159%C<3*+.%/3&<199Q+.CQ.9&*:#.(
!

W*#*I@#*/I(!##@9N.(%/(/@D":6&9% C:"#6&(3*#\$(ABDE(|cc(

!

) * * "%+,-().(/012\$,34(2#(5 ',%6(7 ! 89(: ,1 ;(<==(
(

B"#&C ,.7 ,+DE -&' ,,\$;\$F.9G.&%\$

P\$6() SU(:&% I&C*(/T(*.(9%86&67(H*&.#5(E#.(&%+6(*.(#%(6M@C*/6(#\$6(%:6&@#*%/(#\$@#(9@".67(#\$6(LDW(\$%N(#%(H*&60(.6/7(686/#7@#@#%(" .6&Q.:@960(@/7(76#6&C*/6(3\$6#\$6&(#%(@++3(%&(76/ ,(\$6(%:6&@#*%/(#\$@#(9@".67(#\$6(LDW(\$%N(#%(H*&65(

U*&.#0(#\$6(9%&&69#(\$6@76&(H*+6./667(#%(16(*+9+"767(#%(" .6(#\$6(@: :&% :&*@#6(.#&"9#"&6.(@/7(8@&*@1+6.5(

```
#include <linux/fs.h>
#include <linux/errno.h>
```

(

"#\$%&'!:7(!M' .>'&@!#,40%>'>!#,!' / . A30'!Y6"!3&0\$&. A(

P\$6/(@/7@#@(.#&"9#"&6(*.(76H*/67(#\$@#(3*+.(#%&6(.%C6(9%/#6M#(H&%C(6@9\$(686/#5(E/(#\$*.(9@.60(*#(3*+.(#%&6(\$6(eE[0(SE[0(*#C6.#@C:0*/%76(/"C16&0(@/7(9%CC@/7(/@C6(@..%9*#@67(3*\$6(\$6(686/#5(P\$6/(#\$6() SU2S^BU2] ePSePFG(C@9&%(*(.9@++670(3\$*9\$(3*+(.6#(" :(\$6(/696..@&,(9%C:%/6/#.0(*+9+"7*/I(@(.#&"9#"&6(/@C67(a686/#.0b(H%&(\$6(:&%I&C(#%(.6/7(7@#@(#%(" .6&Q.:@965(

```
struct data_t {
    u32 uid;
    u32 pid;
    u64 ts;
    unsigned long inode_num;
    char comm[TASK_COMM_LEN];
};
BPF_PERF_OUTPUT(events);
```

(

"#\$%&'!:75)!X.-.!*-&%4-%&'!.,>!Y%11'&!-0!6.@@!FR' , -@!#,!F/ . A30'!Y6"!6&0\$&. A(

_6M#(*.(#\$6(LDW2SB]) ^ (C@9&%0(3\$*9\$(.:69*H*6.(3\$*9\$(LDW(\$%N(#\$*.(:&% I&C(3*+(16(@##@9\$67(#%5(P\$6(9%&&69#(\$%N(/@C6(@/7(@&I"C6/#.(@&6(76#6&C*/67(1 ,(+%%N*/I(@#(\$6(9%&&6.:%/7*/I(LDW(\$%N(6/#&,(*/(a*+9+"76<+*/"M<+.C2\$%%N276H.5\$b0(3\$*9\$(3@.(

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*\$(ABDE| c=(
!

!
7*.9"..67(6@&+*6&5(P\$*.(:&%I&@C(3*+(@##@9\$(#(#\$6*/%762:6&C*..%/(LDW(\$%N0(@/7(*#(3*+(
16@1+6(#%(6M@C*/6(#\$6*/%76(.#&"9#"&6(@/7(#\$6(:6&C*..%/(C@.N5(

```
LSM_PROBE(inode_permission, struct inode *inode, int mask) {
```

```
(  
"$%&'!:7D)!*3'4#1+#,$!-; '!8*9!M00I!-0!L@'!#;!F/.A3@'!Y6"!6&0$&.A(  
  
( _6M#*(.($6(9%76($@#(&"/.(3$6/($$*(LDW($%%N(H*&6.5(E#(*/*#@+*d6.(@(.#&"9#"&6(H%&  
686/#(7@#(@/7(#$6/(*/8%N6.($6( )SU($6+:6&(H"/9#%*/(1:H2I6#29"&&6/#2"*72I*7FG0(.#%&*/I(  
%/+,(#$6(+%36&(1*#.(#$@#(9%/#@*/($6(eE[5(P$*.(.(/6(%H(C@/,( )SU($6+:6&(H"/9#%*/.($$@#(  
#$6(N6&/6+(C@N6.(@8@*+@1+6(#%( )SU(:&%I&@C.(+*N6($$*(./6(Ff&6II0(!"I".#(>?>?G5(  
  
U%++%3*/I($$*(.(@/77(.#&*/I0(eE[2UELP^B0(3$*9$*(./%#(T5(E#*(.(@(:+@96$%+76&  
#$@#(3*+16("67(1,(S,$$%/(#%(. "1.*#"#6(+%I*9*/#%($6(:&%I&@C0(76:6/7*/I(%/(:%:##%/.(  
:@..67(#%($6(S,$$%/(.9&*:#5(  

```

```
struct data_t data = {};  
u32 uid = bpf_get_current_uid_gid();  
UID_FILTER
```

```
(  
"$%&'!:7E)!* '--#,$!%3!-; '!L0X!"#0-'&!#;!F/.A3@'!Y6"!6&0$&.A(  
  
( P$6(:&%I&@C($6/(:&6:@&6.(#%(. $%:(7@#@(#%("6&Q.:@96(1,(X"6&,*/I(@/7(.#%&*/I(  
*/H%&C@#%*/(@1%"#$6(9"&&6/#(eE[0(SE[0($*C6.#@C:0*/%76(/"C16&0(@/7(9%CC@/75(E#($@.(  
@996..(#%($6*/%76(.#&"9#"&6(@/7(@/,(%#$6&(@&I"C6/#.($$@#(@&6(@(:&#(%H($6(LDW($%%N5(((  

```

```
data.uid = uid;  
data.pid = bpf_get_current_pid_tgid();  
data.ts = bpf_ktime_get_ns();  
data.inode_num = inode->i_ino;  
bpf_get_current_comm(&data.comm, sizeof(data.comm));
```

```
(  
"$%&'!:7J)!?000'4-#,$!FR',-!X.-.!#;!F/.A3@'!Y6"!6&0$&.A(  
  
( P$6(7@#@(*.(+:@967*/(@/(a686/#.b(1"HH6&($$@#("6&Q.:@96(9@/(@996..5(P$6(C6#$%7*(.  
9@+67(a:6&H2."1C*#b(169@".6(*#(76:6/7.(%/(@(.:69*+@1"HH6&(9@+67(@a:6&H&*/*I(1"HH6&0b(  

```

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(| cJ(

!
3\$*9\$(*.(9%CC%/+,(".67(#%(I@#\$6&(L*/"M(:6&H%&C@/96(C6#&*9.(H&%C(#\$6(N6&/6+5(U*/@++ ,0(
#\$6(:&%I&@C(&6#"&/.(@(:6&C*..*%/(6&&%&0(&6."+#*/I(*/#\$6(:&%96..(16*/I(76/*67(@996..(%(#\$6(
*/%765(

```
events.perf_submit(ctx, &data, sizeof(data));  
return -EPERM;
```

(
"\$%&'!:7K)!FR',-!X.-.!*%2A#@#@#0,!.,>!:44'@!X',#.C!#,!F/.A3C'!Y6"!6&0\$&.A(

B"0\$H/ ,.DE-&' , \$F?6597\$E' .*-6\$

(P\$6(S,\$\$%/(:%&#*%/(%H(#\$6(:&%I&@C(*.(3\$@#(#\$6(" .6&(6M69"#6.5(] /+,(N6,(:%&#*%/(.%H(
#\$6(S,\$\$%/(.9&*:#(&6(9%86&67(\$6&6\(#\$6H"++(:&%I&@C(9@/(16(&68*6367(@#(#\$6(6/7(%H(#\$*.(
@:::6/7*M5(

P\$6(T(:&%I&@C("%#+*/67(6@&+*6&(*.(6C167767(*/#%(#\$6(S,\$\$%/(.9&*:#0(16*/I(@..*I/67(
#%(#\$6(8@&*@1+6(a1:H2#6M#b(@.(@C"+#*Q+*/6(.#&*/I5(

```
bpf_text = ""  
#include <linux/fs.h>  
#include <linux/errno.h>  
...
```

(
"\$%&'!:7P)!FA2'>>#,\$!-; '!Y6"!6&0\$&.A!#,!F/.A3C'!Y??!*4-(

(P\$6(S,\$\$%/(.9&*:#(7*69#+,(C%7*H*6.(#\$6(T(:&%I&@C(16H%&6(*#(*.(9%C:*+67(@/7(
+%@7675(E/(#\$6(/*: :6#(16+%30(S,\$\$%/(&6: +@96.(#\$6(aeE [2UELP^Bb(.#&*/I(*/#\$6(T(
:&%I&@C(3*#\$(@ (1&@/9\$*/I(.#@#6C6/#(\$#@#(3*++(@++%3(*%/76(@996..(H%&(@++(eE [.)4I)50(#\$6(
%/6(:@..67(#%(\$6(S,\$\$%/(.9&*:#(@.(@/(@&I"C6/#5(

```
bpf_text = bpf_text.replace('UID_FILTER',  
    'if (uid != %s) { return 0; }' % args.uid)
```

(
"\$%&'!:7Q)!*%2@-#-%-#,\$!"#C-'&@!#,!F/.A3C'!Y??!*4-(

(P\$6(T(:&%I&@C(*.(#\$6/(9%C:*+67(@/7(+%@767(*/#%(\$6(N6&/6+(1,(* /8%N*/I(#\$6()) SUFG(
H"/9#*%/(#\$@#(*.(:@&#(%H(#\$6(a199b(S,\$\$%/(+*1&@&,5(

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*\$(ABDE(c`(!

!

```
b = BPF(text=bpf_text)
```

(

"#\$%&'!:7U)!?0A3#\$, \$!., >!80.>#, \$!Y6"!6&0\$&. A!#, !F/. A3C'!Y? ?!*4-!

(P\$6(S,\$\$%/(.9&*:#9@/(#\$6/(@996..(\$6(686/#7@#@1,(%:6/*I(\$6(a686/#.b(1"HH6&(\$6@#(3@.(76H*/67*(#\$6(T(:&%I&@C5(

```
b["events"].open_perf_buffer(print_event)
while 1:
    try:
        b.perf_buffer_poll();
    except KeyboardInterrupt:
        exit()
```

(

"#\$%&'!:7(V)!600#, \$!10&!FR', -@!#, !F/. A3C'!Y? ?!*4-!

P\$6(H%+% 3*/I(*.(@/(6M@C:+6(%H(\$6(.9&*:#*(/(!: :6/7*M(!16*/I(*8%N67(#(76/,(*/%76(@996..(H&%C(eE[(;>c=5(- \$6/(#\$6(" .6&(@##6C: #.(#%(DDR(#(\$6(.6&86&(3 \$6&6(\$\$.(:&% I&@C*.(&"//*/I0(\$6("%#: "#(*.(@.(H%+% 3.(FC%7*H*67(H%&(&6@7@1*+*#, G'(
(

```
# ./mac_deny_inode_access.py -u 1000
TIME(s)      COMM      UID    PID    INODE    MESSAGE
0.000000000 (systemd) 1000   5330   42508571 Deny: inode_permission
hook
0.000038826 (systemd) 1000   5330   42508571 Deny: inode_permission
hook
0.000046959 (systemd) 1000   5330   42508571 Deny: inode_permission
hook
0.023633858 sshd      1000   5338   42508571 Deny: inode_permission
hook
0.023823824 sshd      1000   5338   42508571 Deny: inode_permission
hook
0.023833802 sshd      1000   5338   42508571 Deny: inode_permission
hook
```

(

"#\$%&'!:7((!)Z%-3%-!0!F/. A3C'!Y? ?!*4-(

!

B"4\$>1+!I3&%-+,\$<;;\$F.9G.&%\$

```
#!/usr/bin/python

from bcc import BPF
from bcc.utils import printb
import argparse
import pwd

def parse_uid(user):
    try:
        result = int(user)
    except ValueError:
        try:
            user_info = pwd.getpwnam(user)
        except KeyError:
            raise argparse.ArgumentTypeError(
                "{0!r} is not valid UID or user entry".format(user))
        else:
            return user_info.pw_uid
    else:
        # Maybe validate if UID < 0 ?
        return result

examples = """examples:
    ./deny_inode_permission -u 1000    # deny all inode permissions for
    UID 1000
    """

parser = argparse.ArgumentParser(
    description="Deny the specified user of any inode
interactions",
    formatter_class=argparse.RawDescriptionHelpFormatter,
    epilog=examples)
parser.add_argument("-u", "--uid", type=parse_uid, metavar='USER',
    required=True, help="trace this UID")
args = parser.parse_args()

bpf_text = """
#include <linux/fs.h>
#include <linux/errno.h>

struct data_t {
    u32 uid;
    u32 pid;
    u64 ts;
    unsigned long inode_num;
    char comm[TASK_COMM_LEN];
};
BPF_PERF_OUTPUT(events);

LSM_PROBE(inode_permission, struct inode *inode, int mask) {

    struct data_t data = {};
```

!

```
u32 uid = bpf_get_current_uid_gid();

UID_FILTER

data.uid = uid;
data.pid = bpf_get_current_pid_tgid();
data.ts = bpf_ktime_get_ns();
data.inode_num = inode->i_ino;
bpf_get_current_comm(&data.comm, sizeof(data.comm));
events.perf_submit(ctx, &data, sizeof(data));
return -EPERM;
}
"""

bpf_text = bpf_text.replace('UID_FILTER',
                             'if (uid != %s) { return 0; }' % args.uid)

b = BPF(text=bpf_text)
#b = BPF(src_file="mac_deny_inode_access.c")

# header
print("%-18s %-16s %-6s %-6s %-12s %-6s" % ("TIME(s)", "COMM", "UID",
"PID", "INODE", "MESSAGE"))

# process event
start = 0
def print_event(cpu, data, size):
    global start
    event = b["events"].event(data)
    if start == 0:
        start = event.ts
        time_s = (float(event.ts - start)) / 1000000000
        print(b"%-18.9f %-16s %-6d %-6d %-12d %s" % (time_s, event.comm,
event.uid, event.pid,
event.inode_num, b"Deny during inode_permission hook"))

# loop with callback to print_event
b["events"].open_perf_buffer(print_event)
while 1:
    try:
        b.perf_buffer_poll()
    except KeyboardInterrupt:
        exit()!
```

(

!

) ** "%+,-(<.(>0,"1()&1,?,1@(<3' ;(8&\$,*1(
(

```
X"*6#2@9#*8#,5.$(
#!/usr/bin/bash

MIN_SLEEP=1
MAX_SLEEP=15
NONROOT_USER=billy
DMZ_IP=10.1.1.1

create_world_writable_file() {

    local tmpfile="/tmp/${RANDOM:-world_writable}"

    date +"%Y-%m-%d %H:%M:%S" type=createwoth comm=touch
user=$NONROOT_USER"
    su - $NONROOT_USER -c "umask 0000 && touch $tmpfile >/dev/null 2>&1"
&& rm -f $tmpfile >/dev/null 2>&1

}

add_world_writable_bit() {

    local tmpfile="$(mktemp)"

    date +"%Y-%m-%d %H:%M:%S" type=addwoth comm=chmod user=$NONROOT_USER"
    su - $NONROOT_USER -c "chmod o+w $tmpfile >/dev/null 2>&1"
    rm -f $tmpfile >/dev/null 2>&1

}

add_suid_bit() {

    local tmpfile="$(mktemp)"

    echo 'whoami' > $tmpfile
    chown $NONROOT_USER $tmpfile
    date +"%Y-%m-%d %H:%M:%S" type=addsuid comm=chmod user=$NONROOT_USER"
    sudo -u $NONROOT_USER chmod u+s $tmpfile >/dev/null 2>&1
    rm -f $tmpfile >/dev/null 2>&1

}

run_suid() {

    local choice=$(shuf -i 0-1 -n 1)

    case $choice in
        0)
            date +"%Y-%m-%d %H:%M:%S" type=runsuid comm=sudo
user=$NONROOT_USER"
            sudo -u $NONROOT_USER sudo id >/dev/null 2>&1
            ;;
        1)
    
```


!

```

    date +"%Y-%m-%d %H:%M:%S" type=runsuid comm=passwd
user=$NONROOT_USER"
    sudo -u $NONROOT_USER passwd -S >/dev/null 2>&1
    ;;
esac
}

ipv4_connect_attempt() {

    local o1=192
    local o2=168
    local o3=10
    local o4=$(shuf -i 8-23 -n 1)
    local port=$(shuf -i 1-61000 -n 1)

    local choice=$(shuf -i 0-1 -n 1)

    case $choice in
        0)
            # tcp
            date +"%Y-%m-%d %H:%M:%S" type=ip4_connect comm=bash
ip=$o1.$o2.$o3.$o4 proto=6 port=$port"
            timeout 15 sudo -u $NONROOT_USER bash -c "echo
>/dev/tcp/$o1.$o2.$o3.$o4/$port 2>/dev/null"
            ;;
        1)
            # udp
            date +"%Y-%m-%d %H:%M:%S" type=ip4_connect comm=bash
ip=$o1.$o2.$o3.$o4 proto=17 port=$port"
            timeout 15 sudo -u $NONROOT_USER bash -c "echo
>/dev/udp/$o1.$o2.$o3.$o4/$port 2>/dev/null"
            ;;
    esac
}

ssh_proxy() {

    local choice=$(shuf -i 0-1 -n 1)
    local port=$(shuf -i 10000-60000 -n 1)

    case $choice in
        0)
            local port_fwd_opt="-L $port:ubuntu.com:443"
            ;;
        1)
            local port_fwd_opt="-D $port"
            ;;
    esac

    date +"%Y-%m-%d %H:%M:%S" type=ssh_proxy comm=ssh
port_fwd_options=$port_fwd_opt"
    sudo -u $NONROOT_USER ssh -n -o ConnectTimeout=5 -o
ConnectionAttempts=1 $port_fwd_opt $DMZ_IP 'id' >/dev/null 2>&1

```

```

!
}

kill_bcc_script() {

    local signo_choice=$(shuf -i 0-1 -n 1)
    local bcc_choice=$(shuf -i 0-4 -n 1)

    case $signo_choice in
        0)
            signo=9
            ;;
        1)
            signo=15
            ;;
    esac

    case $bcc_choice in
        0)
            bcc_script="mac_fileperms"
            ;;
        1)
            bcc_script="mac_suidexec"
            ;;
        2)
            bcc_script="mac_sshlisteners"
            ;;
        3)
            bcc_script="mac_socketconnections"
            ;;
        4)
            bcc_script="mac_killtasks"
            ;;
    esac

    date +"%Y-%m-%d %H:%M:%S" type=kill comm=pkill user=root signo=$signo
    target=$bcc_script
    pkill -f -$signo $bcc_script >/dev/null 2>&1
}

while :
do

    interval=$(shuf -i $MIN_SLEEP-$MAX_SLEEP -n 1)
    sleep $interval || exit 1

    choice=$(shuf -i 0-6 -n 1)
    case $choice in
        0)
            create_world_writable_file
            ;;
        1)
            add_world_writable_bit
            ;;
        2)

```

W**I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*\$(ABDE(| =>(!

!

```
    add_suid_bit
    ;;
3)
    run_suid
    ;;
4)
    ipv4_connect_attempt
    ;;
5)
    ssh_proxy
    ;;
6)
    kill_bcc_script
    ;;
esac
done
exit 0!
```

!

W**I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*\$(ABDE(=c(

!

) * * "%+,-(=.(820\$&"(=2+"(2#(A+'1\$" ' '(
(

```
32'451''06!  
#include <unistd.h>  
#include <fcntl.h>  
#include <stdio.h>  
#include <stdlib.h>  
#include <string.h>  
#include <time.h>  
#include <sys/time.h>  
  
/*  
 * mdstress: Rudimentary metadata stress tester  
 *  
 * Creates a file, writes a small string to it,  
 * then deletes it in a tight loop.  
 *  
 * *** This program does not validate input! ***  
 *  
 * Arguments:  
 *   @file:           The file to create and delete  
 *   @total-inodes:   How many times the inode should be  
created/deleted  
 *   @rate-per-second: How many times per second it should be  
created/deleted  
 */  
  
int main(int argc, char *argv[]) {  
  
    int fd;  
    long loops;  
    long delay_ns;  
    double begin;  
    double end;  
    struct timeval tv;  
    struct timespec next;  
    ssize_t num_written;  
    char data[9] = "mdstress";  
  
    if (argc < 4 || strcmp(argv[1], "--help") == 0) {  
        printf("usage: %s file total-inodes rate-per-  
second\n",  
            argv[0]);  
        return 0;  
    }  
  
    loops = strtol(argv[2], NULL, 10);  
    delay_ns = 1000000000 / strtol(argv[3], NULL, 10);  
  
    /* For calculating sleep time per loop */  
    clock_gettime(CLOCK_MONOTONIC, &next);  
  
    /* For measuring elapsed wall time at end of execution */  
    gettimeofday(&tv, NULL);  
    begin = tv.tv_sec * 1000000 + tv.tv_usec;
```

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*#\$(ABDE(|==(

!

```
while (loops-- > 0) {
    next.tv_nsec += delay_ns;
    next.tv_sec += next.tv_nsec / 1000000000;
    next.tv_nsec %= 1000000000;

    fd = open(argv[1], O_RDWR | O_CREAT,
               S_IRUSR | S_IWUSR | S_IRGRP | S_IWGRP
               |
               S_IROTH | S_IWOTH);
    if (fd == -1)
        perror("open");

    num_written = write(fd, data, strlen(data));
    if (num_written == -1)
        perror("write");

    if (close(fd) == -1)
        perror("close");

    if (unlink(argv[1]) == -1)
        perror("unlink");

    clock_nanosleep(CLOCK_MONOTONIC, TIMER_ABSTIME, &next,
NULL);
}

gettimeofday(&tv, NULL);
end = tv.tv_sec * 1000000 + tv.tv_usec;

printf("Total inodes: %s | Inodes per second: %s | Time
elapsed: %f\n",
       argv[2], argv[3], (end - begin) / 1000000.0);

return 0;
}!
```

!

W*#*I@#*/I(!##@9N.(%/(@D":6&9%C:"#6&(3*#\$(ABDE(=J(

!

) ** "%+,-(B.(C"1:2\$D(/0%,%6'(E\$,2\$(12(1&*D34,(<"%&;A3\$D(
(

/6#3%&N2#"/*I.5.\$(

#!/bin/bash

tcpkali has a client-server model. Some of these tunings
are intended for a server, and others for a client. However,
for simplicity's sake all, the settings were applied to every
device participating in the benchmark, whether server or
client.

N=100000

sysctl fs.file-max=\$((10000+2*N))
sysctl net.ipv4.tcp_max_orphans=\$((N))

For load-generating clients.
sysctl net.ipv4.ip_local_port_range="10000 65535"
sysctl net.ipv4.tcp_tw_reuse=1

#For server
sysctl net.core.somaxconn=16384

#For NIC
ifconfig em1 txqueuelen 5000

sysctl net.core.netdev_max_backlog=2000
sysctl net.ipv4.tcp_max_syn_backlog=8192

Do this manually so it applies to the bash session
ulimit -n 65536

!

W*#*I@#*/I(!##@9N.(%/(@D":6&9% C:"#6&(3*#\$(ABDE(| =`(
!

!

) * * "%+,-(F.(<"%&; A3\$D(! " '041' (

(

^@9\$(M\$:+(&6."#+(*.(@/(@86&@I6(%H(#\$*&#,(&" / .(% / (#\$6(/%76(H%&(#\$6(I*86/(9%/H*I" &@#*% /5(
(

M\$:+(P*C6(^+@:.67(FD69%/7.G(
_@C6(_%/QABDE(A6&/6+(ABDE(N6&/6+0(_%(D9&*:#.(ABDE(N6&/6+0(!++()) TT(D9&*:#.(
_%76(;(882.26	882.32	882.21
_%76(>(896.69	895.10	891.45
_%76(c(888.22	888.60	887.67
_%76(=(886.10	885.93	886.01
_%76(J(878.59	878.67	878.37
_%76(`(887.85	888.08	889.28
_%76(K(876.81	876.30	876.44
_%76(h(878.12	878.79	878.47

(

M\$:+(f*I@H+:%.(
_@C6(_%/QABDE(A6&/6+(ABDE(N6&/6+0(_%(D9&*:#.(ABDE(N6&/6+0(!++()) TT(D9&*:#.(
_%76(;(711.22	711.17	711.26
_%76(>(699.77	701.02	703.89
_%76(c(706.44	706.15	706.88
_%76(=(708.14	708.27	708.21
_%76(J(714.19	714.12	714.37
_%76(`(706.74	706.56	705.60
_%76(K(715.65	716.06	715.95
_%76(h(714.59	714.06	714.32

(

^@9\$(C7.#&6..(&6."#+(*.(@/(@86&@I6(%H(#\$*&#,(&" / .(% / (#\$6(/%76(H%&(#\$6(I*86/(9%/H*I" &@#*% /5(
(

(

C7.#&6..(P*C6(^+@:.67(F;??0???(*/%76.(4(;?0???(:6&(.69%/7G(
_@C6(?``=(3*#\$(/%(.9&*:#.(?``=(3<(C@92H*+6:6&C.(?````(3<(C@92H*+6:6&C.(
_%76(;(10.00	10.00	10.00
_%76(>(10.00	10.00	10.00
_%76(c(10.00	10.00	10.00
_%76(=(10.00	10.00	10.00
_%76(J(10.00	10.00	10.00
_%76(`(10.00	10.00	10.00
_%76(K(10.00	10.00	10.00
_%76(h(10.00	10.00	10.00

(

(

(

(

!

C7.#&6..(P*C6(^+@:.67(FJ??0???(*/%76.(4(J??0???(:6&(.69%/7G(
_@C6(?``=(3*#\$(/%(.9&*:#.(?``=(3<(C@92H*+6:6&C.(?````(3<(C@92H*+6:6&C.(
_%76(;	13.61	13.88	15.19
_%76(>)	13.40	13.72	15.46
_%76(c	13.66	14.14	15.67
_%76(=)	14.87	15.76	16.28
_%76(J	14.85	14.93	15.69
_%76(`	13.06	13.82	15.35
_%76(K	13.98	15.05	16.16
_%76(h	15.92	14.72	16.07

(

C7.#&6..(P*C6(^+@:.67(F;0??0???(*/%76.(4(;??0???(:6&(.69%/7G(
_@C6(?``=(3*#\$(/%(.9&*:#.(?``=(3<(C@92H*+6:6&C.(?````(3<(C@92H*+6:6&C.(
_%76(;	27.18	27.06	29.54
_%76(>)	26.93	28.24	29.98
_%76(c	26.77	26.39	30.80
_%76(=)	28.67	29.19	30.21
_%76(J	28.76	29.36	31.15
_%76(`	26.05	26.13	29.45
_%76(K	27.38	28.79	30.57
_%76(h	29.63	30.23	31.81

(

#9:N@+*(FC@92.N9%/ /69#*%/.(/%#(+@767G(
T+*6/#(D6&86&.(P*C6(T%/ /69#*%/.(S6&(D69%/7(D"996..H"+(T%/ /69#*%/.(E76@+(W@M(T%/ /69#*%/.(
_%76(;	_%76(>)	30	1500	46422	45000
_%76(;	_%76.(q>Qcr	30	3000	92843	90000
_%76(;	_%76.(q>Q=r	30	4500	139255	135000
_%76(;	_%76.(q>QJr	30	6000	185594	180000
_%76(;	_%76.(q>Q`r	30	7500	232106	225000
_%76(;	_%76.(q>QKr	30	9000	276026	270000
_%76(;	_%76.(q>Qhr	30	10500	305430	315000

(

#9:N@+*(FC@92.N9%/ /69#*%/.(+@767G(
T+*6/#(D6&86&.(P*C6(T%/ /69#*%/.(S6&(D69%/7(D"996..H"+(T%/ /69#*%/.(E76@+(W@M(T%/ /69#*%/.(
_%76(;	_%76(>)	30	1500	46415	45000
_%76(;	_%76.(q>Qcr	30	3000	92819	90000
_%76(;	_%76.(q>Q=r	30	4500	139230	135000
_%76(;	_%76.(q>QJr	30	6000	185608	180000
_%76(;	_%76.(q>Q`r	30	7500	232063	225000
_%76(;	_%76.(q>QKr	30	9000	275750	270000
_%76(;	_%76.(q>Qhr	30	10500	297864	315000

!