บทที่ 5

การทดสอบระบบตรวจจับการบุกรุก และการปรับปรุง

ในบทนี้จะกล่าวถึงการทดสอบ และการปรับปรุงระบบตรวจจับการบุกรุกที่ได้พัฒนาขึ้น ในส่วนแรกจะกล่าวถึงสภาพแวดล้อมที่ใช้ในการทดสอบ ส่วนต่อมาจะเป็นการทดสอบระบบตรวจจับการบุกรุกและการปรับปรุงรูปแบบการจัดเก็บข้อมูลในแฟ้มข้อมูลฝึกสอนระบบเพื่อให้ระบบตรวจจับการบุกรุกทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น จากนั้นจะเป็นการพัฒนาระบบตรวจจับการบุกรุกเพื่อให้สามารถทำงานกับระบบปฏิบัติการเวอร์ชันที่สูงขึ้นได้แล้วนำผลการทดสอบมาสร้างกราฟ หลังจากนั้นจะกล่าวถึงประสิทธิภาพในการทำงานของระบบปฏิบัติการเมื่อมีการทำงานของระบบตรวจจับการบุกรุกอยู่เบื้องหลังเพื่อวิเคราะห์ผลกระทบที่อาจจะมีต่อระบบ และในส่วนสุดท้ายจะเป็นการสรุปผลการทดสอบ

5.1 สภาพแวดล้อมในการทดสอบระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุกพัฒนาขึ้นบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ซึ่งมีสภาพแวดล้อมในการทดสอบเป็นดังตาราง 5.1

ตาราง 5.1 รายละเอียดของระบบปฏิบัติการลินุกซ์เรดแฮ็ทที่ใช้ในการทดสอบ

Linux RedHat release	6.1
machine processor architecture name	i686
release name	Cartman
kernel version	2.2.12-20

5.2 การทดสอบระบบตรวจจับการบุกรุก

การทดสอบระบบตรวจจับการบุกรุกบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 มีวัตถุประสงค์ ขอบเขต ข้อจำกัด และวิธีการทดสอบ ดังต่อไปนี้

วัตถุประสงค์ในการทดสอบ เพื่อทดสอบการทำงานของระบบตรวจจับการบุก-รุกที่พัฒนาขึ้นว่ามีความสามารถแยกแยะการทำงานแบบปกติหรือการบุกรุกระบบได้หรือไม่

ขอบเขตในการทดสอบ แบ่งการทดสอบระบบตรวจจับการบุกรุกออกเป็น 2 ส่วน คือ

1. ทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือทดสอบที่ได้เก็บพฤติ-กรรมการทำงานของโปรเซสไว้ในแฟ้มข้อมูลฝึกสอนระบบ

2. ทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือทดสอบที่ไม่ได้เก็บพฤติ-กรรมการทำงานของโปรเซสไว้ในแฟ้มข้อมูลฝึกสอนระบบ

การทดสอบทั้ง 2 ส่วนนี้แบ่งกลุ่มการทดสอบออกเป็น 4 กลุ่ม คือ กลุ่ม DoS กลุ่ม root compromise กลุ่ม miscellany และกลุ่ม system command ซึ่งมีรายละเอียดตามที่ได้กล่าวไว้ในหัวข้อ 2.7.2 ของบทที่ 2 ซึ่งความผิดพลาดที่เกิดขึ้นจากการทดสอบแบ่งออกเป็น 2 ประเภท ดังนี้

1. ถ้าระบบตรวจจับการบุกรุกไม่สามารถตรวจจับการบุกรุกจากเครื่องมือในกลุ่ม DoS กลุ่ม root compromise และกลุ่ม miscellany ได้แล้วความผิดพลาดที่เกิดขึ้นนี้เป็นความผิดพลาดแบบการตัดสินทางลบ (false negative) เนื่องจากระบบตรวจจับการบุกรุกวิเคราะห์ข้อมูลแล้วตัดสินว่าไม่ได้เกิดจากพฤติกรรมหรือการกระทำที่เป็นการบุกรุกระบบทั้งที่ในความเป็นจริงแล้วเหตุการณ์หรือพฤติกรรมนั้นเป็นรูปแบบของการบุกรุก

2. ถ้าระบบตรวจจับการบุกรุกรายงานว่าการทดสอบโดยใช้เครื่องมือในกลุ่ม system command เป็นการบุกรุกระบบแล้ว ความผิดพลาดที่เกิดขึ้นนี้เป็นความผิดพลาดแบบการตัดสินทางบวก (false positive) เนื่องจากระบบตรวจจับการบุกรุกวิเคราะห์ข้อมูลแล้วตัดสินว่ารูปแบบข้อมูลนั้นเป็นพฤติกรรมการบุกรุกทั้งที่ในความเป็นจริงแล้วรูปแบบข้อมูลนั้นเกิดจากพฤติ-กรรมการใช้งานตามปกติหรือได้รับอนุญาตจากระบบ

ข้อจำกัดในการทดสอบ

1. ระบบตรวจจับการบุกรุกที่พัฒนาขึ้นนี้เป็นแบบ host-based IDS ดังนั้นเครื่องมือที่ใช้ทดสอบจึงเป็นแบบ host-based และผู้บุกรุกระบบที่ตรวจจับได้นั้นคือ ผู้ใช้งานภายในระบบเท่านั้น

2. เนื่องจากระบบปฏิบัติการลินุกซ์เรดแฮ็ทสร้างแฟ้มข้อมูลแบบ flush memory เมื่อในระบบมีโปรเซสเป็นจำนวนมากจะมีผลกระทบกับการสร้างแฟ้มข้อมูล ซึ่งเป็นข้อมูลนำเข้าของระบบตรวจจับการบุกรุก เมื่อระบบตรวจจับการบุกรุกเปิดแฟ้มข้อมูลเพื่อนับความถี่ของซิสเท็มคอลจะทำให้ได้ความถี่น้อยกว่าปกติจึงมีผลต่อความผิดพลาดทางบวกและความผิดพลาดทางลบในการทำงาน

วิธีการทดสอบ

1. เปิดคอมพิวเตอร์เครื่องที่ใช้ระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 และให้ระบบตรวจจับการบุกรุกทำงาน

2. ล็อกอินเข้าทำงานเป็นผู้ใช้งานทั่วไปในระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ผ่านเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows XP แล้วทดสอบการทำงานของระบบตรวจจับการบุกรุกตามขอบเขตการทดสอบที่ได้อธิบายไว้

ตาราง 5.2 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 14 พฤศจิกายน 2547 เวลา 13.21-14.46 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	4	1
dns	5	4	1
inets	5	4	1
innetd	5	5	0
local	5	2	3
lohost	5	4	1
pid	5	4	1
smack	5	5	0
stream	5	5	0
รวม	45	37	8

ตาราง 5.3 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 14 พฤศจิกายน 2547 เวลา 10.10-11.54 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	4	1
backd	5	5	0
blow	5	2	3
cfing	5	5	0

ตาราง 5.3 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 14 พฤศจิกายน 2547 เวลา 10.10–11.54 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
chm	5	5	0
cwho	5	5	0
dir	5	4	1
font	5	5	0
hide	5	5	0
lrs	5	5	0
man	5	1	4
mayday	5	4	1
md	5	4	1
minb	5	5	0
mrem	5	4	1
ovas	5	4	1
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	87	13

ตาราง 5.4 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดลองวันที่ 14 พฤศจิกายน 2547 เวลา 8.32–9.57 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	4	1
adv2	5	5	0
iw	5	5	0

ตาราง 5.4 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดลองวันที่ 14 พฤศจิกายน 2547 เวลา 8.32-9.57 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
ker	5	4	1
kern	5	4	1
lib	5	3	2
lin	5	4	1
lo	5	5	0
lsb	5	5	0
lsof	5	3	2
ptrac	5	5	0
redman	5	3	2
rh	5	5	0
sdi	5	5	0
sor	5	4	1
spider	5	4	1
suex	5	4	1
sur	5	5	0
sxp	5	5	0
xwho	5	4	1
รวม	100	86	14

ตาราง 5.5 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 15 พฤศจิกายน 2547 เวลา 8.42-23.18 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0

ตาราง 5.5 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 15 พฤศจิกายน 2547 เวลา 8.42-23.18 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	4	1
chmod	5	3	2
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	5	0
du	5	4	1
gcc	5	5	0
grep	5	5	0
gunzip	5	3	2
hostname	5	4	1
id	5	5	0
kill	5	4	1
last	5	5	0
ln	5	5	0
ls	5	4	1
man	5	5	0
mkdir	5	5	0
more	5	5	0
mv	5	5	0
netstat	5	2	3

ตาราง 5.5 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 15 พฤศจิกายน 2547 เวลา 8.42-23.18 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
passwd	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	4	1
su	5	5	0
syslogd	5	3	2
tar	5	5	0
top	5	5	0
touch	5	5	0
uname	5	5	0
useradd	5	4	1
vi	5	5	0
wc	5	5	0
whereis	5	3	2
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	202	18

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.2 ถึงตาราง 5.5 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.6

ตาราง 5.6 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.2 ถึงตาราง 5.5

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	82.22
miscellany	87.00
root compromise	86.00
system command	91.82

จากตาราง 5.6 จะเห็นว่าค่าร้อยละของความถูกต้องของการตรวจจับในกลุ่มเครื่องมือบุกรุกระบบที่หาได้จากอินเทอร์เน็ตยังมีร้อยละของการทำงานที่ถูกต้องที่ต่ำอยู่จึงพยายามจัดเก็บพฤติกรรมการทำงานของโปรเซสใหม่ โดยนำข้อมูลจากแฟ้มหลักฐานการบุกรุกที่ถูกเก็บไว้ในสารบบ /testit/evidence/ ซึ่งระบบตรวจจับการบุกรุกตัดสินว่ามีพฤติกรรมการทำงานในข่ายการบุกรุกระบบทั้งที่โดยแท้จริงแล้วเป็นการทำงานตามปกติในระบบมาดำเนินการเก็บข้อมูลเพิ่มลงไปในแฟ้มข้อมูลฝึกสอนระบบ โดยใช้วิธีการแบบเดิมซึ่งได้นำเสนอไว้แล้วในหัวข้อ 4.4 ของบทที่ 4 ซึ่งจะทำให้ได้พฤติกรรมการทำงานของโปรเซสที่ครอบคลุมมากยิ่งขึ้น หลังจากนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกด้วยเครื่องมือทดสอบอย่างเดียวกันใหม่ ผลการทดสอบระบบตรวจจับการบุกรุกหลังจากปรับปรุงแฟ้มข้อมูลฝึกสอนระบบแล้วเป็นดังตาราง 5.7 ถึงตาราง 5.10

ตาราง 5.7 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 13.12-14.34 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	5	0
inets	5	4	1
innetd	5	3	2
local	5	4	1
lohost	5	5	0
pid	5	4	1

ตาราง 5.7 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 13.12-14.34 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
smack	5	5	0
stream	5	5	0
รวม	45	40	5

ตาราง 5.8 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 10.06-11.49 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	4	1
backd	5	4	1
blow	5	4	1
cfing	5	5	0
chm	5	4	1
cwho	5	5	0
dir	5	5	0
font	5	5	0
hide	5	4	1
lrs	5	5	0
man	5	2	3
mayday	5	5	0
md	5	5	0
minb	5	5	0
mrem	5	4	1
ovas	5	4	1
pingb	5	5	0

ตาราง 5.8 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 10.06-11.49 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	90	10

ตาราง 5.9 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 8.24-9.54 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	5	0
adv2	5	5	0
iw	5	4	1
ker	5	4	1
kern	5	4	1
lib	5	4	1
lin	5	4	1
lo	5	5	0
lsb	5	5	0
lsof	5	4	1
ptrac	5	5	0
redman	5	4	1
rh	5	5	0
sdi	5	5	0

ตาราง 5.9 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 17 พฤศจิกายน 2547 เวลา 8.24-9.54 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
sor	5	4	1
spider	5	4	1
suex	5	4	1
sur	5	5	0
sxp	5	5	0
xwho	5	5	0
รวม	100	90	10

ตาราง 5.10 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 18 พฤศจิกายน 2547 เวลา 9.11-23.58 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	4	1
chmod	5	4	1
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	4	1

ตาราง 5.10 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 18 พฤศจิกายน 2547 เวลา 9.11-23.58 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
du	5	5	0
gcc	5	5	0
grep	5	5	0
gunzip	5	4	1
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	5	0
man	5	5	0
mkdir	5	5	0
more	5	5	0
mv	5	4	1
netstat	5	3	2
passwd	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
su	5	5	0
syslogd	5	4	1
tar	5	5	0
top	5	5	0
touch	5	5	0

ตาราง 5.10 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ ทดสอบวันที่ 18 พฤศจิกายน 2547 เวลา 9.11-23.58 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	212	8

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.7 ถึงตาราง 5.10 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.11

ตาราง 5.11 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกหลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.7 ถึงตาราง 5.10

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	88.89
miscellany	90.00
root compromise	90.00
system command	96.36

จากตาราง 5.11 จะเห็นว่าค่าร้อยละของความถูกต้องของการตรวจจับโดยรวมดีขึ้น โดยมีค่าร้อยละของความถูกต้องส่วนใหญ่สูงถึงร้อยละเก้าสิบ ดังนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกใหม่โดยใช้เครื่องมือบุกรุกระบบจากอินเทอร์เน็ตที่ไม่ได้จัดเก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ ผลการทดสอบเป็นดังตาราง 5.12 ถึงตาราง 5.15

ตาราง 5.12 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 9.07-9.35 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
irc	5	2	3
mmap	5	3	2
ptr	5	0	5
shut	5	0	5
std	5	2	3
wts	5	3	2
รวม	30	10	20

ตาราง 5.13 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 10.03-10.38 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
exp	5	4	1
exu	5	3	2
host	5	3	2
umnt	5	4	1
vuln	5	3	2
wtm	5	2	3
รวม	30	19	11

ตาราง 5.14 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 8.24-8.56 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
elf	5	3	2
k	5	4	1

ตาราง 5.14 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 19 พฤศจิกายน 2547 เวลา 8.24-8.56 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
km	5	3	2
mog	5	3	2
spl	5	3	2
vul	5	3	2
รวม	30	19	11

ตาราง 5.15 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดลองวันที่ 19 พฤศจิกายน 2547 เวลา 13.08-22.46 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
apm	5	5	0
ash	5	5	0
bsh	5	5	0
cmp	5	4	1
df	5	5	0
diff	5	5	0
diff3	5	3	2
echo	5	5	0
find	5	3	2
gzip	5	3	2
ifconfig	5	3	2
pwd	5	5	0
sleep	5	4	1
sort	5	5	0
stty	5	4	1
tcsh	5	5	0

ตาราง 5.15 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดลองวันที่ 19 พฤศจิกายน 2547 เวลา 13.08-22.46 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
unzip	5	4	1
userdel	5	3	2
w	5	5	0
zcat	5	5	0
zip	5	4	1
รวม	105	90	15

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.12 ถึงตาราง 5.15 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.16

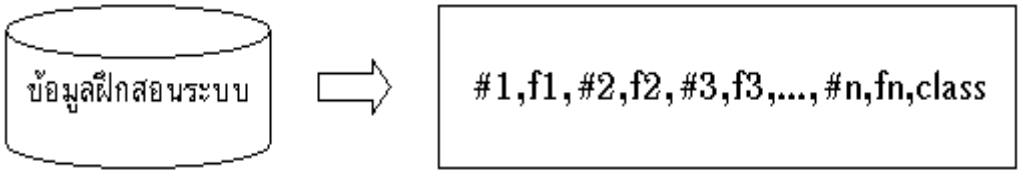
ตาราง 5.16 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.12 ถึงตาราง 5.15

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	33.33
miscellany	63.33
root compromise	63.33
system command	85.71

ผลการทดสอบโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บข้อมูลไว้ในแฟ้มข้อมูลฝึกสอนระบบแสดงให้เห็นว่า ความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกยังมีประสิทธิภาพต่ำ และการปรับปรุงแฟ้มข้อมูลฝึกสอนระบบโดยใช้วิธีการนำพฤติกรรมการทำงานของโปรเซสมาเปรียบเทียบกันเพื่อเลือกหมายเลขซิสเท็มคอลที่ใช้เป็นตัวแทนพฤติกรรมการทำงานของโปรเซสก็เป็นเรื่องยากที่จะเลือกหมายเลขซิสเท็มคอลที่ทำให้เกิดความแตกต่างกันอย่างชัดเจนระหว่างกลุ่มการทำงานแบบปกติและกลุ่มการทำงานแบบผิดปกติเพราะจะต้องนำพฤติกรรมการทำงานของโปรเซสทั้งหมดมาเปรียบเทียบกันใหม่เพื่อเลือกหมายเลขซิสเท็มคอลที่เหมาะสม ปัญหาที่เกิดขึ้นนี้นอกจากจะเป็นความยุ่งยากในการเลือกตัวแทนที่เหมาะสมแล้วยังต้องปรับปรุง

source code ของระบบตรวจจับการบุกรุกเพื่อให้การนับความถี่ของซิสเท็มคอลมีรูปแบบเดียวกันกับแฟ้มข้อมูลฝึกสอนระบบด้วยเพราะถ้ารูปแบบข้อมูลไม่ตรงกันจะทำให้โปรแกรม TiMBL ไม่สามารถทำงานแยกประเภทข้อมูลได้ นอกจากนี้การเลือกหมายเลขซิสเท็มคอลมาเป็นตัวแทนจำเป็นต้องทิ้งซิสเท็มคอลบางรายการไปซึ่งข้อมูลที่ถูกทิ้งไปนี้ก็เป็นพฤติกรรมการทำงานอย่างหนึ่งที่โปรเซสได้แสดงออกมาซึ่งหมายความว่าข้อมูลบางอย่างที่เป็นลักษณะเฉพาะตัวของโปรเซสได้หายไป และจากความสามารถของโปรแกรม TiMBL ที่สามารถรองรับลักษณะประจำตัวของข้อมูลที่ไม่เกี่ยวข้องกันเป็นจำนวนมากได้นำไปสู่การสร้างข้อมูลฝึกสอนระบบแบบใหม่

ข้อมูลฝึกสอนระบบแบบใหม่ ข้อมูลฝึกสอนระบบแบบใหม่เป็นการเก็บข้อมูลโดยใช้ความถี่ของซิสเท็มคอลทั้งหมดที่เกิดจากการทำงานของโปรเซสแทนการเลือกหมายเลขซิสเท็มคอลบางตัวมาใช้เป็นตัวแทนพฤติกรรมการทำงานของโปรเซส ข้อมูลฝึกสอนระบบแบบใหม่มีรูปแบบการจัดเก็บตามภาพประกอบ 5.1



ภาพประกอบ 5.1 รูปแบบการเก็บข้อมูลในแฟ้มข้อมูลฝึกสอนระบบแบบใหม่

จากภาพประกอบ 5.1 ความหมายของสัญลักษณ์ที่ใช้เป็นดังนี้

- #n หมายถึง หมายเลขซิสเท็มคอลตามการกำหนดของระบบปฏิบัติการ
- fn หมายถึง จำนวนครั้งที่โปรเซสเรียกใช้งานซิสเท็มคอลหมายเลขที่ n ในการทำงานครั้งนั้น
- class หมายถึง ชื่อคำสั่งของระบบปฏิบัติการหรือโปรแกรมบุกรุกระบบ ในกรณีที่เป็นคำสั่งของระบบปฏิบัติการจะมีชื่อคลาสเป็นชื่อของคำสั่งนั้น แต่ถ้าเป็นโปรแกรมบุกรุกระบบจะกำหนดให้ใช้ชื่อคลาสว่า “abnormal”

การสร้างข้อมูลฝึกสอนระบบแบบใหม่มีขั้นตอนคล้ายคลึงกับการสร้างข้อมูลฝึกสอนระบบแบบเก่าที่ได้นำเสนอในหัวข้อ 3.4 และ 4.4 ของบทที่ 3 และ 4 ตามลำดับ แต่จะมีความแตกต่างกันที่ข้อมูลฝึกสอนระบบแบบใหม่เก็บข้อมูลที่เกิดขึ้นทั้งหมดไว้เป็นพฤติกรรมการทำงานของโปรเซส ตัวอย่างข้อมูลที่จัดเก็บไว้ในแฟ้มข้อมูลฝึกสอนระบบแบบใหม่เป็นดังภาพประกอบ 5.2 เมื่อสร้างข้อมูลฝึกสอนระบบแบบใหม่โดยการเก็บข้อมูลที่เกิดขึ้นทั้งหมดเสร็จ

เรียบร้อยแล้วจึงดำเนินการทดสอบระบบตรวจจับการบุกรุกใหม่ด้วยวิธีการแบบเดียวกันกับที่ได้ทดสอบระบบตรวจจับการบุกรุกที่ใช้ข้อมูลฝึกสอนระบบแบบเก่า

```
1,0,2,0,3,24,4,14,5,28,6,27,7,0,8,0,9,0,10,0,11,2,12,0,13,3,14,0,15,0,16,...,abnormal
1,0,2,1,3,8,4,1,5,16,6,11,7,0,8,0,9,0,10,0,11,2,12,0,13,0,14,0,15,0,16,0,17,...,abnormal
1,0,2,1,3,8,4,2,5,20,6,11,7,0,8,0,9,0,10,0,11,2,12,0,13,0,14,0,15,0,16,0,17,...,abnormal
1,0,2,1,3,8,4,2,5,20,6,11,7,0,8,0,9,0,10,0,11,2,12,0,13,0,14,0,15,0,16,0,17,0,...,abnormal
1,0,2,1,3,8,4,2,5,20,6,11,7,0,8,0,9,0,10,0,11,2,12,0,13,0,14,0,15,0,16,0,17,0,...,abnormal
1,0,2,1,3,8,4,1,5,16,6,11,7,0,8,0,9,0,10,0,11,2,12,0,13,0,14,0,15,0,16,0,17,...,abnormal
1,1,2,0,3,2,4,3,5,4,6,1,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,0,18,...,abnormal
1,1,2,0,3,2,4,3,5,4,6,1,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,0,...,abnormal
1,1,2,0,3,2,4,3,5,4,6,1,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,0,...,abnormal
1,1,2,0,3,2,4,3,5,4,6,1,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,0,...,abnormal
1,0,2,0,3,24,4,14,5,28,6,27,7,0,8,0,9,0,10,0,11,2,12,0,13,3,14,0,15,0,16,0,...,abnormal
1,0,2,0,3,24,4,14,5,28,6,27,7,0,8,0,9,0,10,0,11,2,12,0,13,3,14,0,15,0,16,0,...,abnormal
                                        ...
1,1,2,0,3,2,4,0,5,7,6,6,7,0,8,0,9,0,10,3,11,1,12,0,13,0,14,0,15,0,16,0,17,...,cc
1,1,2,0,3,6,4,2,5,13,6,12,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,...,cat
1,1,2,0,3,3,4,0,5,12,6,10,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,1,16,0,17,...,chmod
1,1,2,0,3,3,4,4,5,14,6,10,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,...,cp
1,0,2,0,3,15,4,1,5,13,6,8,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,...,grotty
1,1,2,0,3,7,4,2,5,5,6,4,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,0,...,gtbl
1,1,2,0,3,1,4,1,5,3,6,2,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,17,...,hostname
1,1,2,0,3,3,4,1,5,12,6,10,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,...,id
1,1,2,0,3,5,4,1,5,14,6,11,7,0,8,0,9,0,10,0,11,1,12,0,13,0,14,0,15,0,16,0,...,ps
1,0,2,0,3,2,4,0,5,4,6,2,7,0,8,0,9,0,10,0,11,1,12,0,13,1,14,0,15,0,16,0,17,...,last
1,1,2,0,3,3,4,1,5,14,6,12,7,0,8,0,9,0,10,0,11,1,12,0,13,1,14,0,15,0,16,0,...,ls
```

ภาพประกอบ 5.2 ตัวอย่างข้อมูลที่ถูกจัดเก็บไว้ในแฟ้มข้อมูลฝึกสอนระบบแบบเก็บข้อมูลที่เกิดขึ้นทั้งหมด

การทดสอบระบบตรวจจับการบุกรุกโดยใช้ข้อมูลฝึกสอนระบบแบบใหม่

ตาราง 5.17 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 24 เมษายน 2548 เวลา 11.41-13.09 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	5	0
inets	5	5	0
innetd	5	5	0

ตาราง 5.17 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 24 เมษายน 2548 เวลา 11.41-13.09 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
local	5	2	3
lohost	5	4	1
pid	5	3	2
smack	5	5	0
stream	5	5	0
รวม	45	39	6

ตาราง 5.18 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 24 เมษายน 2548 เวลา 15.15-16.54 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	5	0
backd	5	5	0
blow	5	2	3
cfing	5	5	0
chm	5	5	0
cwho	5	5	0
dir	5	5	0
font	5	5	0
hide	5	5	0
lrs	5	4	1
man	5	0	5
mayday	5	5	0
md	5	5	0
minb	5	5	0

ตาราง 5.18 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 24 เมษายน 2548 เวลา 15.15-16.54 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
mrem	5	3	2
ovas	5	5	0
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	89	11

ตาราง 5.19 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 24 เมษายน 2548 เวลา 8.43-10.06 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	4	1
adv2	5	5	0
iw	5	5	0
ker	5	5	0
kern	5	5	0
lib	5	4	1
lin	5	5	0
lo	5	5	0
lsb	5	5	0
lsof	5	4	1
ptrac	5	4	1
redman	5	5	0
rh	5	4	1

ตาราง 5.19 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 24 เมษายน 2548 เวลา 8.43-10.06 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
sdi	5	5	0
sor	5	5	0
spider	5	3	2
suex	5	5	0
sur	5	3	2
sxp	5	4	1
xwho	5	4	1
รวม	100	89	11

ตาราง 5.20 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 25 เมษายน 2548 เวลา 9.02-23.43 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	4	1
date	5	5	0

ตาราง 5.20 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 25 เมษายน 2548 เวลา 9.02-23.43 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
du	5	2	3
gcc	5	5	0
grep	5	5	0
gunzip	5	4	1
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	3	2
man	5	5	0
mkdir	5	5	0
more	5	5	0
mv	5	5	0
netstat	5	5	0
passwd	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
su	5	5	0
syslogd	5	5	0
tar	5	5	0
top	5	5	0
touch	5	2	3
uname	5	5	0

ตาราง 5.20 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 25 เมษายน 2548 เวลา 9.02–23.43 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
useradd	5	5	0
vi	5	4	1
wc	5	5	0
whereis	5	3	2
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	207	13

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.17 ถึงตาราง 5.20 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.21

ตาราง 5.21 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้แฟ้มข้อมูลฝึกสอนระบบแบบใหม่ในตาราง 5.17 ถึงตาราง 5.20

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	86.67
miscellany	89.00
root compromise	89.00
system command	94.09

จากตาราง 5.21 จะเห็นว่าค่าร้อยละของความถูกต้องของการตรวจจับในกลุ่มเครื่องมือบุกรุกระบบที่หาได้จากอินเทอร์เน็ตยังมีร้อยละของความถูกต้องที่ต่ำอยู่จึงพยายามจัดเก็บพฤติกรรมการทำงานของโปรเซสใหม่ให้มีความครอบคลุมมากยิ่งขึ้นโดยใช้วิธีการแบบเดียวกันกับที่ได้นำเสนอไปแล้วในหัวข้อ 5.2 หลังจากนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกด้วยเครื่องมือทดสอบอย่างเดียวกันใหม่ ผลการทดสอบระบบตรวจจับการบุกรุกหลังจากปรับปรุงแฟ้มข้อมูลฝึกสอนระบบแบบใหม่แล้วแสดงดังตาราง 5.22 ถึงตาราง 5.25

ตาราง 5.22 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 9.33-10.52 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	5	0
inets	5	5	0
innetd	5	5	0
local	5	3	2
lohost	5	4	1
pid	5	4	1
smack	5	5	0
stream	5	5	0
รวม	45	41	4

ตาราง 5.23 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 22.06-23.52 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	5	0
backd	5	5	0
blow	5	5	0
cfing	5	5	0
chm	5	5	0
cwho	5	4	1
dir	5	5	0
font	5	5	0
hide	5	5	0

ตาราง 5.23 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 22.06-23.52 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
lrs	5	5	0
man	5	3	2
mayday	5	4	1
md	5	5	0
minb	5	5	0
mrem	5	4	1
ovas	5	5	0
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	95	5

ตาราง 5.24 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 14.10-15.27 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	5	0
adv2	5	5	0
iw	5	5	0
ker	5	5	0
kern	5	5	0
lib	5	5	0
lin	5	4	1

ตาราง 5.24 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 27 เมษายน 2548 เวลา 14.10-15.27 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
lo	5	4	1
lsb	5	5	0
lsof	5	5	0
ptrac	5	4	1
redman	5	5	0
rh	5	4	1
sdi	5	5	0
sor	5	5	0
spider	5	4	1
suex	5	5	0
sur	5	4	1
sxp	5	5	0
xwho	5	5	0
รวม	100	94	6

ตาราง 5.25 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 28 เมษายน 2548 เวลา 8.37-23.12 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0

ตาราง 5.25 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 28 เมษายน 2548 เวลา 8.37-23.12 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
cc	5	5	0
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	5	0
du	5	4	1
gcc	5	5	0
grep	5	5	0
gunzip	5	5	0
hostname	5	4	1
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	3	2
man	5	5	0
mkdir	5	5	0
more	5	5	0
mv	5	5	0
netstat	5	3	2
passwd	5	5	0

ตาราง 5.25 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 28 เมษายน 2548 เวลา 8.37-23.12 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
su	5	5	0
syslogd	5	5	0
tar	5	5	0
top	5	5	0
touch	5	5	0
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	214	6

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.22 ถึงตาราง 5.25 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.26

ตาราง 5.26 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกหลังจากปรับปรุงแฟ้มข้อมูลฝึกสอนระบบแบบใหม่ในตาราง 5.22 ถึงตาราง 5.25

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	91.11
miscellany	95.00
root compromise	94.00
system command	97.27

จากตาราง 5.26 จะเห็นว่าค่าร้อยละของความถูกต้องในการตรวจจับโดยใช้ข้อมูลฝึกสอนระบบแบบใหม่ที่ได้ปรับปรุงแล้วมีค่ามากกว่าร้อยละเก้าสิบซึ่งเป็นที่น่าพอใจ ดังนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกใหม่โดยใช้เครื่องมือบุกรุกระบบจากอินเทอร์เน็ตที่ไม่ได้จัดเก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ ผลการทดสอบเป็นดังตาราง 5.27 ถึงตาราง 5.30

ตาราง 5.27 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 29 เมษายน 2548 เวลา 9.04-9.36 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
irc	5	3	2
mmap	5	5	0
ptr	5	5	0
shut	5	0	5
std	5	5	0
wts	5	4	1
รวม	30	22	8

ตาราง 5.28 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 29 เมษายน 2548 เวลา 14.28-14.54 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
exp	5	4	1
exu	5	4	1
host	5	5	0
umnt	5	5	0
vuln	5	4	1
wtm	5	5	0
รวม	30	27	3

ตาราง 5.29 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 29 เมษายน 2548 เวลา 11.10-11.37 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
elf	5	5	0
k	5	4	1
km	5	5	0
mog	5	4	1
spl	5	4	1
vul	5	4	1
รวม	30	26	4

ตาราง 5.30 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 30 เมษายน 2548 เวลา 9.07-17.49 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
apm	5	5	0
ash	5	5	0

ตาราง 5.30 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 30 เมษายน 2548 เวลา 9.07–17.49 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bsh	5	4	1
cmp	5	5	0
df	5	4	1
diff	5	5	0
diff3	5	4	1
echo	5	5	0
find	5	5	0
gzip	5	4	1
ifconfig	5	4	1
pwd	5	5	0
sleep	5	4	1
sort	5	5	0
stty	5	5	0
tcsh	5	4	1
unzip	5	5	0
userdel	5	4	1
w	5	5	0
zcat	5	5	0
zip	5	4	1
รวม	105	96	9

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.27 ถึงตาราง 5.30 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.31

ตาราง 5.31 ค่าร้อยละของความถูกต้องจากผลการทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.27 ถึงตาราง 5.30

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	73.33
miscellany	90.00
root compromise	86.67
system command	91.43

จากตาราง 5.31 แสดงให้เห็นว่าการปรับเปลี่ยนรูปแบบการจัดเก็บข้อมูลฝึกสอนระบบทำให้การทำงานของระบบตรวจจับการบุกรุกมีประสิทธิภาพมากยิ่งขึ้น แม้ว่าผลการตรวจ-จับโปรแกรมบุกรุกระบบในกลุ่ม denial of service ที่ไม่ได้จัดเก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบจะมีอัตราความถูกต้องของการทำงานประมาณร้อยละเจ็ดสิบก็ตาม แต่เนื่องจากโปรแกรมบุกรุกระบบในกลุ่มนี้ทำให้ระบบปฏิบัติการลินุกซ์เรดแฮ็ทไม่สามารถทำงานต่อไปได้ ซึ่งเมื่อระบบปฏิบัติการหยุดทำงานโปรเซสอื่น ๆ ที่ทำงานอยู่ก็ไม่สามารถทำงานได้ตามไปด้วย ดังนั้นจึงถือว่าระบบตรวจจับการบุกรุกหลังจากเปลี่ยนแปลงรูปแบบการจัดเก็บข้อมูลฝึกสอนระบบมีการทำงานเป็นที่น่าพอใจ

ตาราง 5.32 และตาราง 5.33 เป็นการนำผลการทดสอบจากการใช้แฟ้มข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่มาเปรียบเทียบกัน

ตาราง 5.32 เปรียบเทียบผลการทดสอบจากการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กลุ่มทดสอบ	ข้อมูลฝึกสอนระบบแบบเก่า		ข้อมูลฝึกสอนระบบแบบใหม่	
	ก่อนปรับปรุง	หลังปรับปรุง	ก่อนปรับปรุง	หลังปรับปรุง
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	82.22	88.89	86.67	91.11
miscellany	87.00	90.00	89.00	95.00
root compromise	86.00	90.00	89.00	94.00
system command	91.82	96.36	94.09	97.27

ตาราง 5.33 เปรียบเทียบผลการทดสอบจากการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่โดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กลุ่มทดสอบ	ข้อมูลฝึกสอนระบบแบบเก่า	ข้อมูลฝึกสอนระบบแบบใหม่
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	33.33	73.33
miscellany	63.33	90.00
root compromise	63.33	86.67
system command	85.71	91.43

ระบบตรวจจับการบุกรุกที่พัฒนาขึ้นใช้งานบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 มีความสามารถในการทำงานตรวจสอบการบุกรุกระบบเป็นที่น่าพอใจกล่าวคือ มีอัตราความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกอยู่ที่ประมาณร้อยละเก้าสิบในขณะที่ระบบปฏิบัติการสามารถให้บริการผู้ใช้งานในระบบได้ตามปกติ ในส่วนต่อไปจะกล่าวถึงการพัฒนาระบบตรวจจับการบุกรุกเพื่อใช้งานกับระบบปฏิบัติการลินุกซ์เรดแฮ็ทในเวอร์ชันที่สูงขึ้น

5.3 การปรับปรุงระบบตรวจจับการบุกรุกเพื่อใช้งานกับระบบปฏิบัติการในเวอร์ชันที่สูงขึ้น

การปรับปรุงระบบตรวจจับการบุกรุกให้ทำงานบนระบบปฏิบัติการลินุกซ์เรด-แฮ็ทในเวอร์ชันที่สูงขึ้น ในการทำวิจัยนี้ได้เลือกใช้ลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และเวอร์ชัน 9.0 โดยที่ข้อมูลของลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และเวอร์ชัน 9.0 แสดงไว้ในตาราง 5.34

ตาราง 5.34 แสดงรายละเอียดของระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และเวอร์ชัน 9.0

Linux RedHat release	7.0	9.0
machine processor architecture name	i686	i686
release name	Guinness	Shrike
kernel version	2.2.16-22	2.4.20-8

ในแต่ละเวอร์ชันของระบบปฏิบัติการลินุกซ์เรดแฮ็ทมีจำนวนซิสเท็มคอลที่กำหนดขึ้นเพื่อใช้งานไม่เท่ากัน สำหรับลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 มีจำนวนซิสเท็มคอล 190

รายการ ลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 มีจำนวนซิสเท็มคอล 221 รายการ ลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 มีจำนวนซิสเท็มคอล 258 รายการ เนื่องจากจำนวนซิสเท็มคอลของระบบปฏิบัติการลินุกซ์เรดแฮ็ทแต่ละเวอร์ชันมีจำนวนไม่เท่ากันจึงตั้งสมมติฐานว่าในการทำงานของโปรเซสอย่างเดียวกันของลินุกซ์เรดแฮ็ทแต่ละเวอร์ชันมีการเรียกใช้งานซิสเท็มคอลแตกต่างกัน เพื่อพิสูจน์สมมติฐานที่ตั้งไว้จึงทดลองเรียกใช้งานคำสั่ง “clear” ซึ่งเป็นคำสั่งล้างจอภาพของระบบปฏิบัติการลินุกซ์ทั้ง 3 เวอร์ชัน หลังจากนั้นจึงนับความถี่ของการเรียกใช้งานซิสเท็มคอลจากการทำงานของคำสั่ง clear ทั้ง 3 เวอร์ชันแล้วนำมาเปรียบเทียบกัน ผลการทดลองแสดงไว้ในตาราง 5.35

ตาราง 5.35 การเรียกใช้งานซิสเท็มคอลของคำสั่ง clear บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0

system call	จำนวนครั้งในการเรียกใช้บน RedHat 6.1	จำนวนครั้งในการเรียกใช้บน RedHat 7.0	จำนวนครั้งในการเรียกใช้บน RedHat 9.0
access	2	2	2
brk	5	5	5
close	4	4	4
execve	1	1	1
exit	1	1	0
exit_group	ไม่มี	ไม่มี	1
fstat	4	4	0
fstat64	ไม่มี	2	4
getpid	1	1	0
ioctl	4	4	5
mmap	9	0	0
mmap2	ไม่มี	0	1
mprotect	4	2	0
munmap	2	2	2
old_mmap	ไม่มี	9	8
open	5	5	5
personality	1	0	0
read	9	11	11
sysctl	0	1	0
set_thread_area	ไม่มี	ไม่มี	1

ตาราง 5.35 การเรียกใช้งานซิสเท็มคอลของคำสั่ง clear บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0 (ต่อ)

system call	จำนวนครั้งในการเรียกใช้บน RedHat 6.1	จำนวนครั้งในการเรียกใช้บน RedHat 7.0	จำนวนครั้งในการเรียกใช้บน RedHat 9.0
uname	0	0	1
write	1	1	1
รวมจำนวน	53	55	52

หมายเหตุ ไม่มี หมายถึง ยังไม่มีการกำหนดซิสเท็มคอลบนระบบปฏิบัติการในเวอร์ชันนั้น

จากตาราง 5.35 ซึ่งแสดงการเรียกใช้งานซิสเท็มคอลของคำสั่ง clear บนลินุกซ์เรดแฮ็ททั้ง 3 เวอร์ชันทำให้ทราบว่าซิสเท็มคอลบางรายการมีการเรียกใช้งานไม่เท่ากันบนระบบปฏิบัติการทั้ง 3 เวอร์ชัน ยิ่งไปกว่านั้นซิสเท็มคอลบางรายการยังไม่มีการกำหนดขึ้นเพื่อใช้งานบนระบบปฏิบัติการในบางเวอร์ชันด้วย ดังนั้นข้อมูลฝึกสอนระบบที่ใช้งานบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 จึงไม่สามารถนำมาใช้งานกับลินุกซ์เรดแฮ็ทเวอร์ชันอื่น ๆ ได้ จึงมีความจำเป็นที่จะต้องเก็บข้อมูลฝึกสอนระบบแยกกันเพื่อใช้งานกับระบบปฏิบัติการลินุกซ์เรดแฮ็ทต่างเวอร์ชันกัน

วิธีการที่ใช้เก็บพฤติกรรมการทำงานของโปรเซสเป็นวิธีการแบบเดียวกันกับที่ได้กล่าวมาแล้ว และใช้รูปแบบการจัดเก็บข้อมูลลงในแฟ้มข้อมูลฝึกสอนระบบแบบเก็บข้อมูลที่เกิดขึ้นทั้งหมด หรือการเก็บข้อมูลแบบใหม่เช่นเดียวกันกับแฟ้มข้อมูลฝึกสอนระบบที่ใช้งานบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 คำสั่งของระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และ 9.0 ที่เลือกมาเก็บพฤติกรรมการทำงานมีดังนี้

คำสั่งของลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0: bash, bc, cal, cat, cc, chgrp, chmod, chown, clear, cp, csh, date, dircolors, du, egrep, gcc, grep, groff, grotty, gtbl, gunzip, hostname, id, kill, ktop, last, less, ln, ls, man, mkdir, more, mv, netstat, passwd, ps, rm, rmdir, sed, sh, sshd, su, syslogd, tar, test, top, touch, tput, troff, uname, unix_chkpwd, useradd, vi, wc, whereis, which, who, whoami, xauth

คำสั่งของลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0: as, bash, bc, cal, cat, cc, cc1, chgrp, chmod, chown, clear, collect2, consoloetype, cp, cpp0, csh, cut, date, dircolors, du, egrep, gcc, grep, groff, grotty, gtbl, gunzip, gzip, hostname, id, kill, last, ld, less, ln,

locale, login, ls, man, mkdir, more, mv, netstat, nroff, ps, rm, rmdir, sed, sh, sshd, stty, syslogd, tar, test, top, touch, tput, troff, uname, useradd, vi, wc, whereis, which, who, whoami

เมื่อเก็บข้อมูลซึ่งเป็นพฤติกรรมการทำงานของโปรเซสไว้ในแฟ้มข้อมูลฝึกสอนระบบเรียบร้อยแล้วจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกด้วยวิธีการอย่างเดียวกันกับการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1

ทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 การทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 มีวัตถุประสงค์ ขอบเขต และข้อจำกัดในการทดสอบเหมือนกันกับการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 จึงขอละไว้ ณ ที่นี้

วิธีการทดสอบ

1. เปิดคอมพิวเตอร์เครื่องที่ใช้ระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และให้ระบบตรวจจับการบุกรุกทำงาน

2. ล็อกอินเข้าทำงานเป็นผู้ใช้งานทั่วไปในระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 ผ่านเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows XP แล้วทดสอบการทำงานของระบบตรวจจับการบุกรุกตามขอบเขตการทดสอบที่ได้อธิบายไว้

การทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 มีลักษณะคล้ายกันกับการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 กล่าวคือเมื่อทดสอบระบบตรวจจับการบุกรุกแล้วพยายามปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ โดยเก็บพฤติ-กรรมการทำงานของโปรเซสให้ครอบคลุมมากขึ้นจะทำให้ประสิทธิภาพในการทำงานของระบบตรวจจับการบุกรุกเพิ่มมากขึ้น ผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 แสดงไว้ในตาราง 5.36 ถึงตาราง 5.43

ตาราง 5.36 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 15.12-16.27 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	0	5
inets	5	5	0
innetd	5	5	0
local	5	5	0
lohost	5	5	0
pid	5	4	1
smack	5	5	0
stream	5	5	0
รวม	45	39	6

ตาราง 5.37 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 21.17-22.53 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	5	0
inets	5	5	0
innetd	5	5	0
local	5	5	0
lohost	5	4	1
pid	5	4	1
smack	5	5	0
stream	5	5	0
รวม	45	43	2

ตาราง 5.38 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 13.07-14.49 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	5	0
backd	5	5	0
blow	5	5	0
cfing	5	5	0
chm	5	5	0
cwho	5	5	0
dir	5	5	0
font	5	5	0
hide	5	5	0
lrs	5	5	0
man	5	3	2
mayday	5	5	0
md	5	4	1
minb	5	5	0
mrem	5	5	0
ovas	5	5	0
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	97	3

ตาราง 5.39 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 13.55-15.41 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	5	0
backd	5	5	0
blow	5	5	0
cfing	5	5	0
chm	5	5	0
cwho	5	5	0
dir	5	5	0
font	5	5	0
hide	5	5	0
lrs	5	5	0
man	5	4	1
mayday	5	5	0
md	5	4	1
minb	5	5	0
mrem	5	5	0
ovas	5	5	0
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	98	2

ตาราง 5.40 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 1 พฤษภาคม 2548 เวลา 9.43-11.29 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	5	0
adv2	5	5	0
iw	5	5	0
ker	5	5	0
kern	5	5	0
lib	5	5	0
lin	5	5	0
lo	5	5	0
lsb	5	4	1
lsof	5	5	0
ptrac	5	5	0
redman	5	5	0
rh	5	5	0
sdi	5	4	1
sor	5	4	1
spider	5	5	0
sur	5	5	0
sxp	5	5	0
xwho	5	4	1
รวม	95	91	4

ตาราง 5.41 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 4 พฤษภาคม 2548 เวลา 9.36-11.27 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	5	0
adv2	5	5	0
iw	5	5	0
ker	5	5	0
kern	5	5	0
lib	5	5	0
lin	5	4	1
lo	5	5	0
lsb	5	4	1
lsof	5	5	0
ptrac	5	5	0
redman	5	5	0
rh	5	5	0
sdi	5	5	0
sor	5	5	0
spider	5	5	0
sur	5	5	0
sxp	5	5	0
xwho	5	4	1
รวม	95	92	3

ตาราง 5.42 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 2 พฤษภาคม 2548 เวลา 8.43-23.36 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	5	0
du	5	5	0
gcc	5	5	0
grep	5	3	2
gunzip	5	5	0
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	5	0
man	5	5	0
mkdir	5	5	0

ตาราง 5.42 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 2 พฤษภาคม 2548 เวลา 8.43-23.36 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
more	5	5	0
mv	5	5	0
netstat	5	3	2
passwd	5	2	3
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
su	5	5	0
syslogd	5	5	0
tar	5	5	0
top	5	5	0
touch	5	5	0
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	213	7

ตาราง 5.43 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 5 พฤษภาคม 2548 เวลา 8.18-23.12 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	4	1
du	5	5	0
gcc	5	5	0
grep	5	5	0
gunzip	5	5	0
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	5	0
man	5	5	0
mkdir	5	5	0

ตาราง 5.43 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 5 พฤษภาคม 2548 เวลา 8.18-23.12 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
more	5	5	0
mv	5	5	0
netstat	5	5	0
passwd	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
su	5	5	0
syslogd	5	5	0
tar	5	5	0
top	5	4	1
touch	5	4	1
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	220	217	3

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.36 ตาราง 5.38 ตาราง 5.40 และตาราง 5.42 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.44

ตาราง 5.44 ค่าร้อยละของความถูกต้องก่อนปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบจากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.36 ตาราง 5.38 ตาราง 5.40 และตาราง 5.42

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	86.67
miscellany	97.00
root compromise	95.79
system command	96.82

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.37 ตาราง 5.39 ตาราง 5.41 และตาราง 5.43 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.45

ตาราง 5.45 ค่าร้อยละของความถูกต้องหลังปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบจากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.37 ตาราง 5.39 ตาราง 5.41 และตาราง 5.43

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	95.56
miscellany	98.00
root compromise	96.84
system command	98.64

จากตาราง 5.45 จะเห็นว่าร้อยละของความถูกต้องมีค่าสูงเกินกว่าร้อยละเก้าสิบ ดังนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกใหม่โดยใช้เครื่องมือบุกรุกระบบจากอินเทอร์เน็ตที่ไม่ได้จัดเก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ ผลการทดสอบเป็นดังตาราง 5.46 ถึงตาราง 5.49

ตาราง 5.46 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 8.36-9.12 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
irc	5	5	0
mmap	5	5	0
ouc	5	0	5
ptr	5	5	0
shut	5	4	1
wts	5	4	1
รวม	30	23	7

ตาราง 5.47 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 10.27-10.58 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
exp	5	4	1
exu	5	5	0
host	5	5	0
umnt	5	4	1
vuln	5	4	1
wtm	5	5	0
รวม	30	27	3

ตาราง 5.48 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 13.42-14.16 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
elf	5	0	5
k	5	5	0

ตาราง 5.48 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 13.42-14.16 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
km	5	5	0
mog	5	5	0
pass	5	5	0
sec	5	4	1
vul	5	5	0
รวม	35	29	6

ตาราง 5.49 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 14.23-23.08 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
apm	5	5	0
ash	5	5	0
bsh	5	5	0
cmp	5	3	2
df	5	5	0
diff	5	4	1
diff3	5	4	1
echo	5	5	0
find	5	4	1
gzip	5	5	0
ifconfig	5	4	1
pwd	5	5	0
sleep	5	5	0
sort	5	5	0
stty	5	5	0

ตาราง 5.49 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 6 พฤษภาคม 2548 เวลา 14.23-23.08 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
tcsh	5	4	1
unzip	5	5	0
userdel	5	5	0
w	5	5	0
zcat	5	5	0
zip	5	4	1
รวม	105	97	8

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.46 ถึงตาราง 5.49 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.50

ตาราง 5.50 ค่าร้อยละของความถูกต้องโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.46 ถึงตาราง 5.49

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	76.67
miscellany	90.00
root compromise	82.86
system command	92.38

เพื่อให้เห็นประสิทธิภาพในการทำงานของระบบตรวจจับการบุกรุกที่เพิ่มมากขึ้น จึงได้นำผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบมาเปรียบเทียบกันในตาราง 5.51

ตาราง 5.51 เปรียบเทียบผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบโดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กลุ่มทดสอบ	ก่อนปรับปรุง	หลังปรับปรุง
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	86.67	95.56
miscellany	97.00	98.00
root compromise	95.79	96.84
system command	96.82	98.64

ทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 การทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 มีวัตถุประสงค์ ขอบเขต และข้อจำกัดในการทดสอบเหมือนกันกับการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 และเวอร์ชัน 7.0 จึงขอละไว้ ณ ที่นี้

วิธีการทดสอบ

1. เปิดคอมพิวเตอร์เครื่องที่ใช้ระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 และให้ระบบตรวจจับการบุกรุกทำงาน

2. ล็อกอินเข้าทำงานเป็นผู้ใช้งานทั่วไปในระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 ผ่านเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows XP แล้วทดสอบการทำงานของระบบตรวจจับการบุกรุกตามขอบเขตการทดสอบที่ได้อธิบายไว้

การทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 มีลักษณะคล้ายกันกับการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 และเวอร์ชัน 7.0 กล่าวคือเมื่อทดสอบระบบตรวจจับการบุกรุกแล้วพยายามปรับปรุงแฟ้มข้อมูลฝึกสอนระบบ โดยเก็บพฤติกรรมการทำงานของโปรเซสให้ครอบคลุมมากขึ้นจะทำให้ประสิทธิภาพในการทำงานของระบบตรวจจับการบุกรุกเพิ่มมากขึ้น ผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 แสดงไว้ในตาราง 5.52 ถึงตาราง 5.59

ตาราง 5.52 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 9.03-10.22 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	4	1
dns	5	5	0
inets	5	5	0
innetd	5	4	1
local	5	5	0
lohost	5	4	1
pid	5	5	0
smack	5	5	0
stream	5	5	0
รวม	45	42	3

ตาราง 5.53 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 8.17-9.41 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
dd	5	5	0
dns	5	5	0
inets	5	5	0
innetd	5	5	0
local	5	4	1
lohost	5	5	0
pid	5	5	0
smack	5	5	0
stream	5	5	0
รวม	45	44	1

ตาราง 5.54 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 10.48-12.36 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	4	1
backd	5	5	0
blow	5	5	0
cfing	5	4	1
chm	5	5	0
cwho	5	4	1
dir	5	5	0
font	5	4	1
hide	5	4	1
lrs	5	4	1
man	5	4	1
mayday	5	5	0
md	5	5	0
minb	5	4	1
mrem	5	4	1
ovas	5	5	0
pingb	5	5	0
purg	5	4	1
sms	5	5	0
sys	5	4	1
รวม	100	89	11

ตาราง 5.55 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 10.02-11.51 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
agro	5	5	0
backd	5	5	0
blow	5	5	0
cfing	5	5	0
chm	5	5	0
cwho	5	4	1
dir	5	5	0
font	5	4	1
hide	5	5	0
lrs	5	5	0
man	5	4	1
mayday	5	5	0
md	5	5	0
minb	5	5	0
mrem	5	4	1
ovas	5	5	0
pingb	5	5	0
purg	5	5	0
sms	5	5	0
sys	5	5	0
รวม	100	96	4

ตาราง 5.56 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 7 พฤษภาคม 2548 เวลา 14.12-15.56 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	4	1
adv2	5	4	1
iw	5	5	0
ker	5	4	1
lib	5	4	1
lin	5	5	0
lo	5	5	0
lsb	5	5	0
lsof	5	5	0
ptrac	5	5	0
redman	5	5	0
rh	5	5	0
sdi	5	5	0
sor	5	4	1
spider	5	5	0
sur	5	5	0
sxp	5	5	0
xwho	5	4	1
รวม	90	84	6

ตาราง 5.57 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 10 พฤษภาคม 2548 เวลา 13.26-15.13 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
adv1	5	5	0
adv2	5	4	1
iw	5	5	0
ker	5	4	1
lib	5	5	0
lin	5	5	0
lo	5	4	1
lsb	5	4	1
lsof	5	5	0
ptrac	5	5	0
redman	5	5	0
rh	5	5	0
sdi	5	5	0
sor	5	5	0
spider	5	5	0
sur	5	5	0
sxp	5	5	0
xwho	5	5	0
รวม	90	86	4

ตาราง 5.58 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 8 พฤษภาคม 2548 เวลา 8.28-23.24 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	5	0
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	5	0
du	5	5	0
gcc	5	4	1
grep	5	5	0
gunzip	5	1	4
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	5	0
ln	5	5	0
ls	5	5	0
man	5	5	0
mkdir	5	5	0

ตาราง 5.58 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ก่อนปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 8 พฤษภาคม 2548 เวลา 8.28-23.24 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
more	5	5	0
mv	5	5	0
netstat	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
syslogd	5	5	0
tar	5	4	1
top	5	5	0
touch	5	5	0
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	210	204	6

ตาราง 5.59 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 11 พฤษภาคม 2548 เวลา 8.22-23.15 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
bash	5	5	0
bc	5	5	0
cal	5	5	0
cat	5	5	0
cc	5	3	2
chgrp	5	5	0
chmod	5	5	0
chown	5	5	0
clear	5	5	0
cp	5	5	0
csh	5	5	0
date	5	5	0
du	5	5	0
gcc	5	5	0
grep	5	5	0
gunzip	5	5	0
hostname	5	5	0
id	5	5	0
kill	5	5	0
last	5	4	1
ln	5	5	0
ls	5	5	0
man	5	5	0
mkdir	5	5	0

ตาราง 5.59 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command หลังปรับปรุงข้อมูลฝึกสอนระบบ ทดสอบวันที่ 11 พฤษภาคม 2548 เวลา 8.22-23.15 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
more	5	5	0
mv	5	5	0
netstat	5	5	0
ps	5	5	0
rm	5	5	0
rmdir	5	5	0
syslogd	5	5	0
tar	5	5	0
top	5	5	0
touch	5	5	0
uname	5	5	0
useradd	5	5	0
vi	5	5	0
wc	5	5	0
whereis	5	5	0
which	5	5	0
who	5	5	0
whoami	5	5	0
รวม	210	207	3

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.52 ตาราง 5.54 ตาราง 5.56 และตาราง 5.58 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.60

ตาราง 5.60 ค่าร้อยละของความถูกต้องก่อนปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบจากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.52 ตาราง 5.54 ตาราง 5.56 และตาราง 5.58

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	93.33
miscellany	89.00
root compromise	93.33
system command	97.14

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.53 ตาราง 5.55 ตาราง 5.57 และตาราง 5.59 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.61

ตาราง 5.61 ค่าร้อยละของความถูกต้องหลังปรับปรุงข้อมูลในแฟ้มข้อมูลฝึกสอนระบบจากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.53 ตาราง 5.55 ตาราง 5.57 และตาราง 5.59

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	97.78
miscellany	96.00
root compromise	95.56
system command	98.57

จากผลการทดสอบที่ได้ในตาราง 5.61 จะเห็นว่าร้อยละของความถูกต้องมีค่ามากกว่าร้อยละเก้าสิบ ดังนั้นจึงทดสอบความสามารถของระบบตรวจจับการบุกรุกใหม่ โดยใช้เครื่องมือบุกรุกระบบจากอินเทอร์เน็ตที่ไม่ได้จัดเก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ ผลการทดสอบเป็นดังตาราง 5.62 ถึงตาราง 5.65

ตาราง 5.62 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม denial of service ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 8.21-8.58 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
mmap	5	5	0
ouc	5	1	4
ptr	5	5	0
shut	5	5	0
wts	5	5	0
รวม	25	21	4

ตาราง 5.63 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม miscellany ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 9.12-9.42 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
exp	5	4	1
exu	5	5	0
host	5	5	0
umnt	5	4	1
vuln	5	5	0
wtm	5	5	0
รวม	30	28	2

ตาราง 5.64 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 13.17-13.52 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
elf	5	4	1
km	5	5	0
mog	5	4	1

ตาราง 5.64 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม root compromise ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 13.17-13.52 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
pass	5	5	0
spl	5	5	0
vul	5	4	1
รวม	30	27	3

ตาราง 5.65 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 14.10-22.57 น.

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
apm	5	5	0
ash	5	5	0
bsh	5	5	0
cmp	5	4	1
df	5	5	0
diff	5	5	0
diff3	5	5	0
echo	5	5	0
find	5	5	0
gzip	5	5	0
ifconfig	5	4	1
pwd	5	5	0
sleep	5	4	1
sort	5	5	0
stty	5	5	0
tcsh	5	5	0
unzip	5	4	1

ตาราง 5.65 การทดสอบระบบตรวจจับการบุกรุกโดยใช้เครื่องมือกลุ่ม system command ทดสอบวันที่ 12 พฤษภาคม 2548 เวลา 14.10-22.57 น. (ต่อ)

เครื่องมือ	จำนวนครั้งที่ทดสอบ	ทำงานถูกต้อง	ทำงานผิดพลาด
userdel	5	4	1
w	5	5	0
zcat	5	4	1
zip	5	5	0
รวม	105	99	6

จากผลการทดสอบระบบตรวจจับการบุกรุกในตาราง 5.62 ถึงตาราง 5.65 สามารถนำมาคำนวณหาร้อยละของความถูกต้องได้ตามตาราง 5.66

ตาราง 5.66 ค่าร้อยละของความถูกต้องโดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบในตาราง 5.62 ถึงตาราง 5.65

กลุ่มทดสอบ	ร้อยละของความถูกต้อง
denial of service	84.00
miscellany	93.33
root compromise	90.00
system command	94.29

เพื่อให้เห็นความสามารถในการทำงานของระบบตรวจจับการบุกรุกบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 ที่เพิ่มมากขึ้นจึงได้นำผลการทดสอบระบบตรวจจับการบุกรุกก่อนและหลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบมาเปรียบเทียบกันในตาราง 5.67

ตาราง 5.67 เปรียบเทียบผลการทดสอบระบบตรวจจับการบุกรุกบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 ก่อนและหลังปรับปรุงแฟ้มข้อมูลฝึกสอนระบบโดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กลุ่มทดสอบ	ก่อนปรับปรุง	หลังปรับปรุง
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	93.33	97.78
miscellany	89.00	96.00
root compromise	93.33	95.56
system command	97.14	98.57

ในส่วนนี้ได้นำเสนอการปรับปรุงระบบตรวจจับการบุกรุกให้สามารถทำงานได้กับระบบปฏิบัติการลินุกซ์เรดแฮ็ทในเวอร์ชันที่สูงขึ้นได้แล้ว ในหัวข้อถัดไปจะนำผลการทดสอบระบบตรวจจับการบุกรุกมานำเสนอในรูปแบบของกราฟเพื่อให้เห็นประสิทธิภาพในการทำงานของระบบตรวจจับการบุกรุกได้ง่ายยิ่งขึ้น

5.4 กราฟแสดงผลการทดสอบ

ก่อนที่จะนำเสนอผลการทดสอบระบบตรวจจับการบุกรุกในรูปแบบของกราฟจะรวบรวมผลการทดสอบการทำงานของระบบตรวจจับการบุกรุกมาแสดงไว้ในตารางเดียวกันแยกตามเวอร์ชันของระบบปฏิบัติการลินุกซ์เรดแฮ็ทดังต่อไปนี้

ตาราง 5.68 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1

กลุ่มทดสอบ	ข้อมูลฝึกสอนระบบแบบเก่า			ข้อมูลฝึกสอนระบบแบบใหม่		
	ก่อนปรับปรุง	หลังปรับปรุง	เครื่องมือที่หามาใหม่	ก่อนปรับปรุง	หลังปรับปรุง	เครื่องมือที่หามาใหม่
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	82.22	88.89	33.33	86.67	91.11	73.33
miscellany	87.00	90.00	63.33	89.00	95.00	90.00
root compromise	86.00	90.00	63.33	89.00	94.00	86.67
system command	91.82	96.36	85.71	94.09	97.27	91.43

ตาราง 5.69 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0

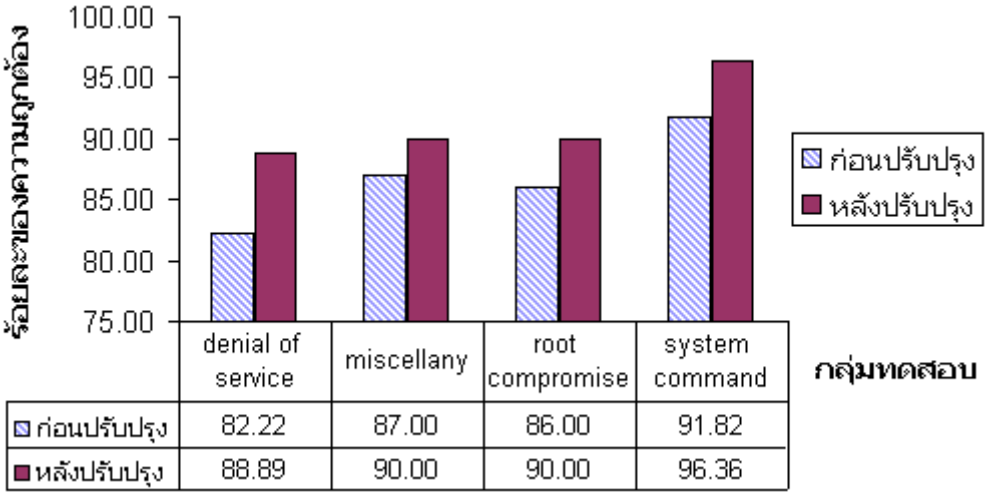
กลุ่มทดสอบ	ข้อมูลฝึกสอนระบบแบบเก็บข้อมูลที่เกิดขึ้นทั้งหมด		
	ก่อนปรับปรุง	หลังปรับปรุง	เครื่องมือที่หามาใหม่
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง
denial of service	86.67	95.56	76.67
miscellany	97.00	98.00	90.00
root compromise	95.79	96.84	82.86
system command	96.82	98.64	92.38

ตาราง 5.70 ผลการทดสอบระบบตรวจจับการบุกรุกทั้งหมดบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0

กลุ่มทดสอบ	ข้อมูลฝึกสอนระบบแบบเก็บข้อมูลที่เกิดขึ้นทั้งหมด		
	ก่อนปรับปรุง	หลังปรับปรุง	เครื่องมือที่หามาใหม่
	ร้อยละของความถูกต้อง	ร้อยละของความถูกต้อง	ร้อยละขอความถูกต้อง
denial of service	93.33	97.78	84.00
miscellany	89.00	96.00	93.33
root compromise	93.33	95.56	90.00
system command	97.14	98.57	94.29

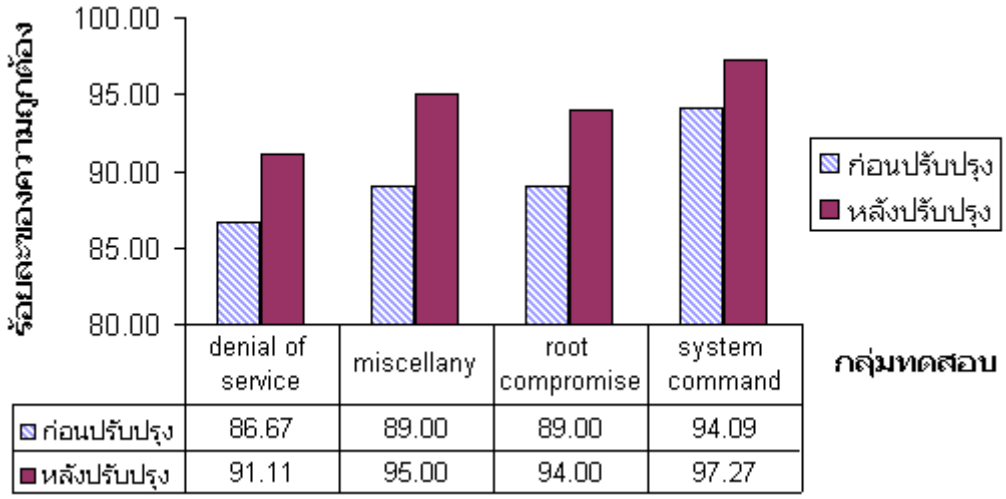
กราฟแสดงผลการทดสอบบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1

กราฟแสดงผลการทดสอบในส่วนนี้เป็นข้อมูลจากตาราง 5.68



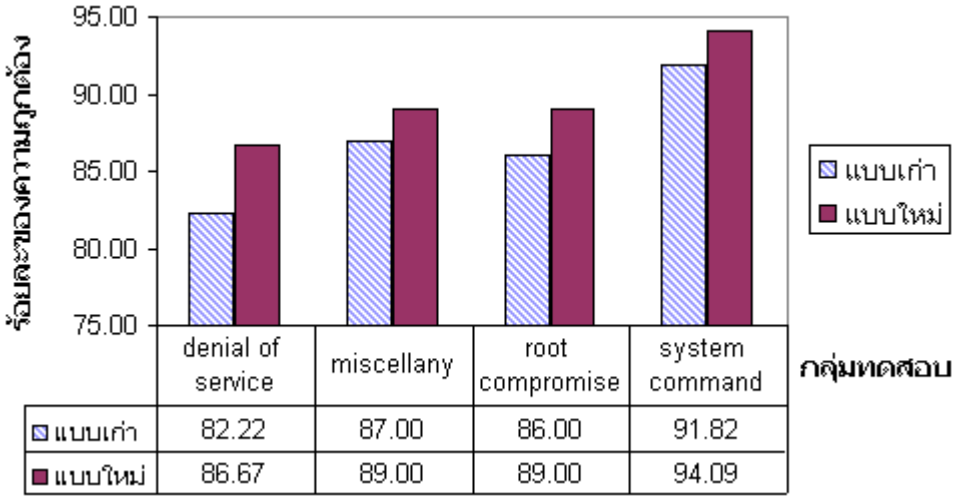
	denial of service	miscellany	root compromise	system command
ก่อนปรับปรุง	82.22	87.00	86.00	91.82
หลังปรับปรุง	88.89	90.00	90.00	96.36

ภาพประกอบ 5.3 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบแบบเก่า โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

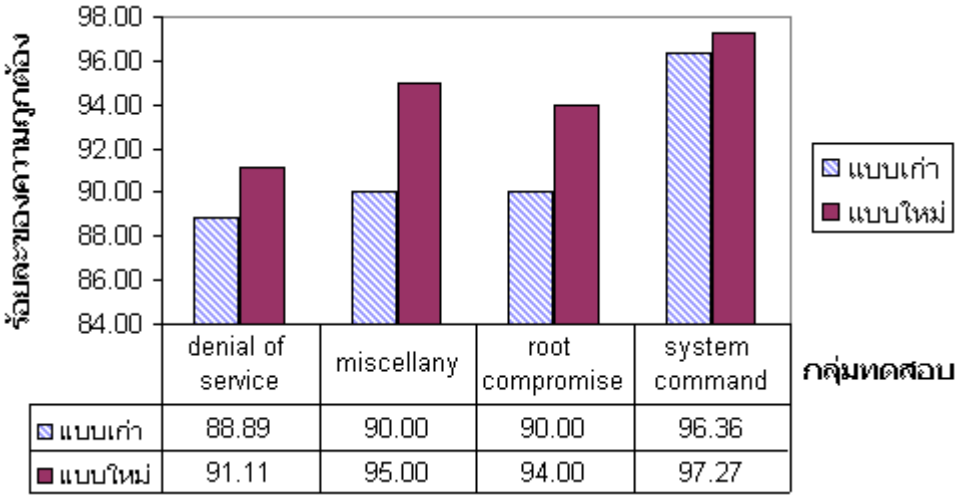


	denial of service	miscellany	root compromise	system command
ก่อนปรับปรุง	86.67	89.00	89.00	94.09
หลังปรับปรุง	91.11	95.00	94.00	97.27

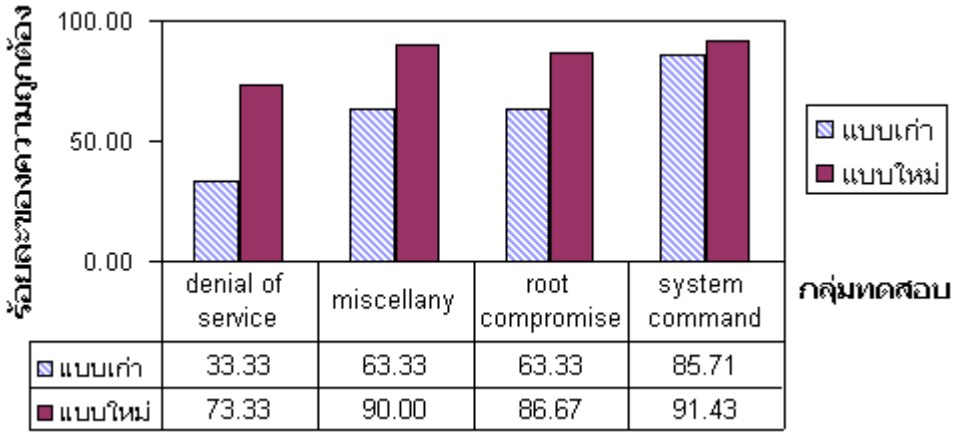
ภาพประกอบ 5.4 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ



ภาพประกอบ 5.5 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ก่อนปรับปรุงข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ



ภาพประกอบ 5.6 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 หลังปรับปรุงข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

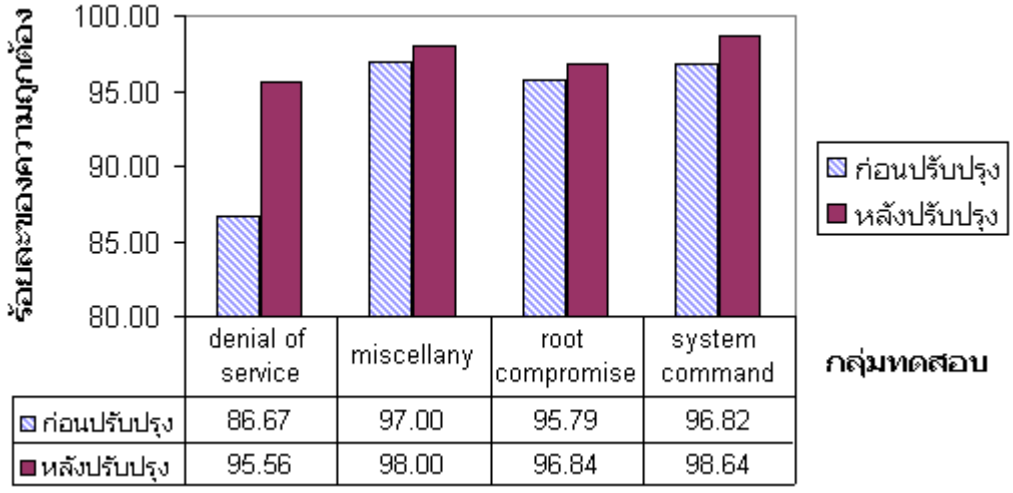


	denial of service	miscellany	root compromise	system command
แบบเก่า	33.33	63.33	63.33	85.71
แบบใหม่	73.33	90.00	86.67	91.43

ภาพประกอบ 5.7 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1ระหว่างการใช้ข้อมูลฝึกสอนระบบแบบเก่ากับแบบใหม่ โดยใช้เครื่องมือบุกรุกระบบที่ไม่ได้เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กราฟแสดงผลการทดสอบบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0

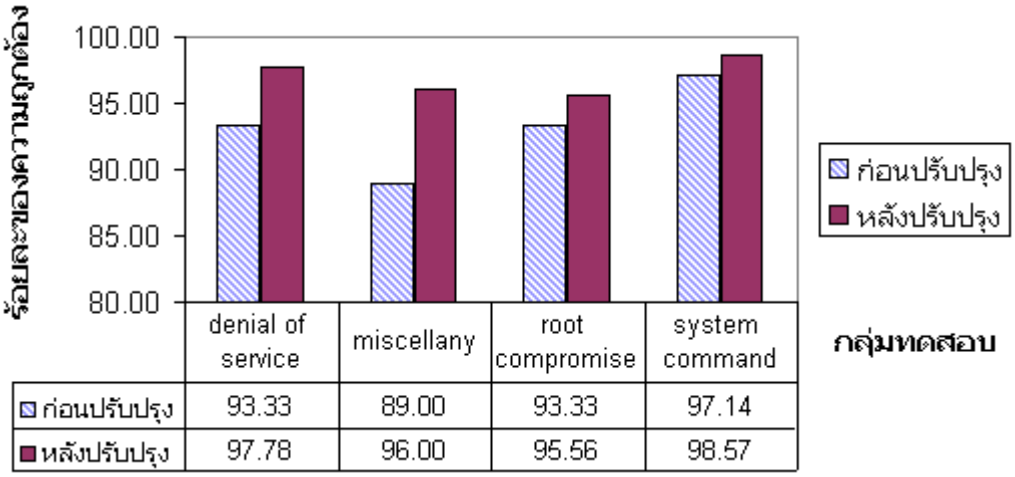
กราฟแสดงผลการทดสอบในส่วนนี้เป็นข้อมูลจากตาราง 5.69



	denial of service	miscellany	root compromise	system command
ก่อนปรับปรุง	86.67	97.00	95.79	96.82
หลังปรับปรุง	95.56	98.00	96.84	98.64

ภาพประกอบ 5.8 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

กราฟแสดงผลการทดสอบบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0
กราฟแสดงผลการทดสอบในส่วนนี้เป็นข้อมูลจากตาราง 5.70



	denial of service	miscellany	root compromise	system command
ก่อนปรับปรุง	93.33	89.00	93.33	97.14
หลังปรับปรุง	97.78	96.00	95.56	98.57

ภาพประกอบ 5.9 กราฟเปรียบเทียบความถูกต้องในการทำงานของระบบตรวจจับการบุกรุก บนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 ก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบ โดยใช้เครื่องมือบุกรุกระบบที่เก็บพฤติกรรมการทำงานไว้ในแฟ้มข้อมูลฝึกสอนระบบ

5.5 ประสิทธิภาพ

ในการทดสอบประสิทธิภาพของระบบตรวจจับการบุกรุกบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0 ได้ใช้โปรแกรม “top” เพื่อแสดงการใช้งานหน่วยความจำและการใช้งานซีพียู (CPU) เปรียบเทียบกันระหว่างในขณะที่มีระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงาน ผลการทดสอบแสดงไว้ในตาราง 5.71 ถึงตาราง 5.73 ตามลำดับ เมื่อนำข้อมูลจากตาราง 5.71 ในส่วนของการใช้งานซีพียูมาสร้างกราฟเปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 จะเป็นไปตามภาพประกอบ 5.10 และเมื่อนำข้อมูลจากตาราง 5.71 ในส่วนของการใช้งานหน่วยความจำมาสร้างกราฟเปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 จะเป็นไปตามภาพประกอบ 5.11 เมื่อนำข้อมูลจากตาราง 5.72 ในส่วนของการใช้งานซีพียูมาสร้างกราฟเปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 จะเป็นไปตามภาพประกอบ 5.12 และเมื่อนำข้อมูลจากตาราง 5.72 ในส่วนของการใช้งานหน่วยความจำมาสร้างกราฟ

เปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 จะเป็นไปตามภาพประกอบ 5.13 เมื่อนำข้อมูลจากตาราง 5.73 ในส่วนของการใช้งานซีพียูมาสร้างกราฟเปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 จะเป็นไปตามภาพประกอบ 5.14 และเมื่อนำข้อมูลจากตาราง 5.73 ในส่วนของการใช้งานหน่วยความจำมาสร้างกราฟเปรียบเทียบการทำงานในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ระบบตรวจจับการบุกรุกไม่ได้ทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 จะเป็นไปตามภาพประกอบ 5.15

ตาราง 5.71 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่

ครั้งที่ตรวจสอบ	การใช้งานซีพียู (%)						การใช้งานหน่วยความจำ (K)		การใช้งาน swap (K)	
	user (ไม่มี IDS)	user (มี IDS)	system (ไม่มี IDS)	system (มี IDS)	idle (ไม่มี IDS)	idle (มี IDS)	(ไม่มี IDS)	(มี IDS)	(ไม่มี IDS)	(มี IDS)
1	0.1	52.2	0.0	47.7	99.8	0.0	40,008	86,420	0	0
2	0.1	50.6	0.0	49.3	99.8	0.0	40,036	124,588	0	3,152
3	0.1	52.0	0.0	47.9	99.8	0.0	40,040	124,828	0	3,148
4	0.1	46.9	0.0	53.0	99.8	0.0	40,048	107,672	0	7,568
5	0.1	49.9	0.0	50.0	99.8	0.0	92,532	107,332	0	7,536
6	0.1	47.5	0.0	51.2	99.8	0.0	92,580	114,368	0	7,476
7	0.1	49.9	0.0	50.0	99.8	0.0	92,580	124,800	0	7,888
8	0.1	45.0	0.0	54.9	99.8	0.0	97,628	124,844	0	7,888
9	0.1	52.0	0.0	47.9	99.8	0.0	97,632	110,652	0	7,888
10	0.1	52.8	0.0	47.1	99.8	0.0	97,632	110,588	0	7,888

หมายเหตุ ฮาร์ดแวร์ : เครื่องไมโครคอมพิวเตอร์ ซีพียู Intel Pentium III 950 MHz หน่วยความจำ 128 MB
ระบบปฏิบัติการ : Linux RedHat release 6.1, release name Cartman, kernel version 2.2.12-20

ตาราง 5.72 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่

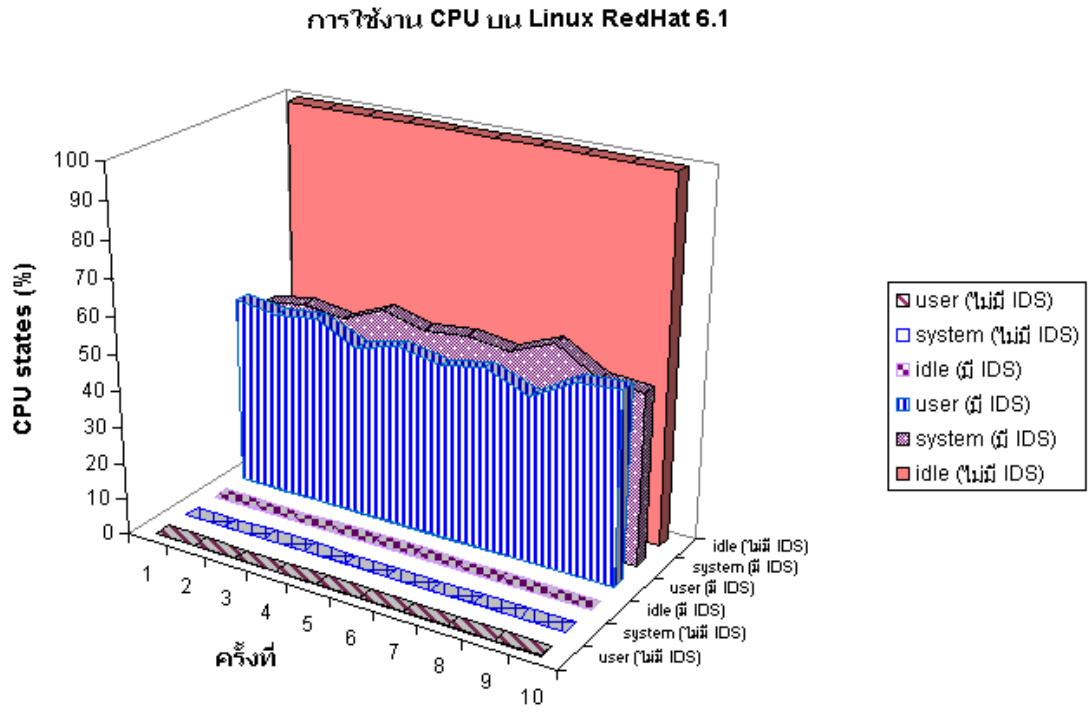
ครั้งที่ตรวจสอบ	การใช้งานซีพียู (%)						การใช้งานหน่วยความจำ (K)		การใช้งาน swap (K)	
	user (ไม่มี IDS)	user (มี IDS)	system (ไม่มี IDS)	system (มี IDS)	idle (ไม่มี IDS)	idle (มี IDS)	(ไม่มี IDS)	(มี IDS)	(ไม่มี IDS)	(มี IDS)
1	0.0	33.5	0.1	66.4	99.8	0.0	61,356	105,732	0	5,836
2	0.0	37.3	0.1	62.6	99.8	0.0	61,360	105,532	0	5,836
3	0.0	34.5	0.1	65.4	99.8	0.0	61,368	105,556	0	5,828
4	0.0	37.4	0.1	62.5	99.8	0.0	61,368	105,512	0	5,828
5	0.0	37.3	0.1	62.6	99.8	0.0	61,380	103,460	0	5,820
6	0.0	33.7	0.1	66.2	99.8	0.0	61,380	103,524	0	5,820
7	0.0	33.5	0.1	66.4	99.8	0.0	61,380	98,748	0	5,816
8	0.0	31.1	0.1	68.8	99.8	0.0	62,340	123,408	0	5,816
9	0.0	34.3	0.1	65.6	99.8	0.0	62,340	124,816	0	6,744
10	0.0	33.0	0.1	66.9	99.8	0.0	62,344	116,664	0	6,744

หมายเหตุ ฮาร์ดแวร์ : เครื่องไมโครคอมพิวเตอร์ ซีพียู Intel Pentium III 950 MHz หน่วยความจำ 128 MB
ระบบปฏิบัติการ : Linux RedHat release 7.0, release name Guinness, kernel version 2.2.16-22

ตาราง 5.73 แสดงการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 ขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานกับขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่

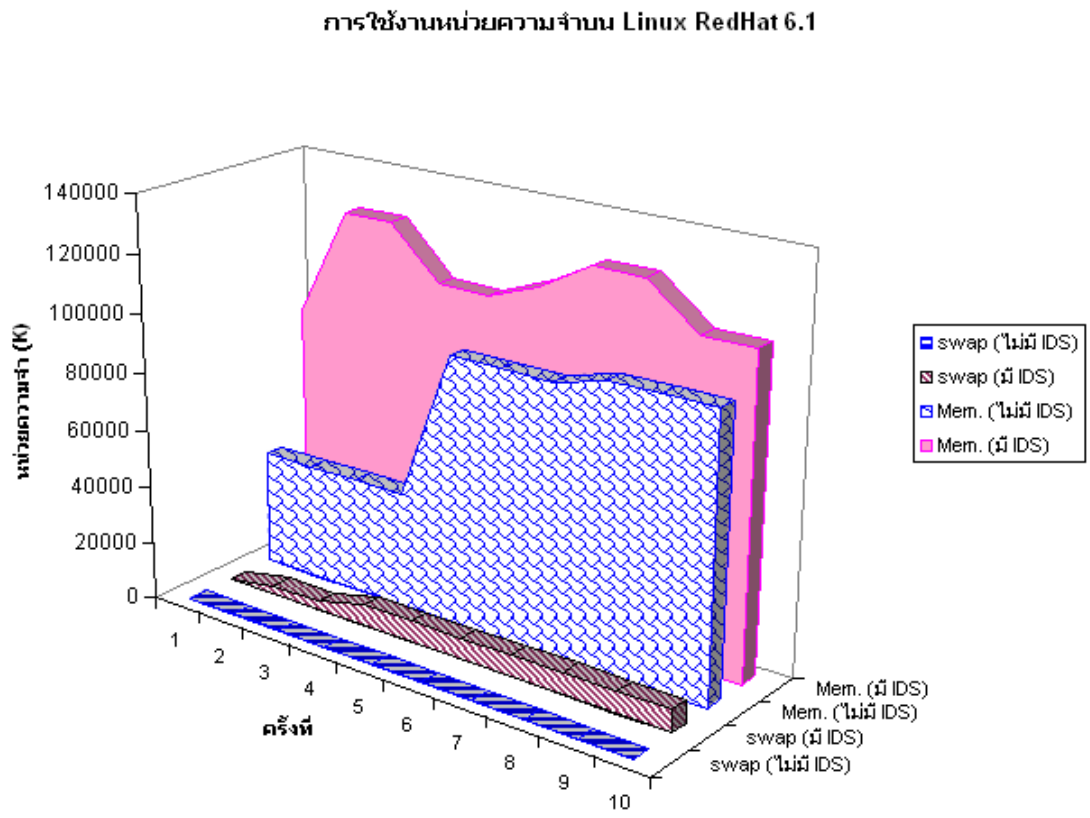
ครั้งที่ตรวจสอบ	การใช้งานซีพียู (%)						การใช้งานหน่วยความจำ (K)		การใช้งาน swap (K)	
	user (ไม่มี IDS)	user (มี IDS)	system (ไม่มี IDS)	system (มี IDS)	idle (ไม่มี IDS)	idle (มี IDS)	(ไม่มี IDS)	(มี IDS)	(ไม่มี IDS)	(มี IDS)
1	0.0	44.2	0.0	55.7	100	0.0	76,696	108,088	0	7,496
2	0.0	38.6	0.0	57.2	100	0.0	123,588	123,584	1,068	41,452
3	0.0	26.3	0.0	32.1	100	40.1	123,588	123,804	1,076	41,804
4	0.0	0.6	0.0	32.8	100	4.1	123,596	123,736	1,076	64,012
5	0.0	0.3	0.0	31.0	100	9.6	123,596	123,804	1,076	63,484
6	0.0	0.2	0.0	0.8	100	98.9	123,332	123,776	1,092	56,092
7	0.0	0.1	0.0	0.7	100	99.1	123,332	123,804	1,092	57,024
8	0.0	0.3	0.0	0.7	100	98.9	123,340	123,800	1,092	56,976
9	0.0	0.1	0.0	0.9	100	99.0	123,076	123,804	1,084	53,884
10	0.0	0.1	0.0	0.7	100	99.0	122,872	123,804	1,652	53,548

หมายเหตุ ฮาร์ดแวร์ : เครื่องไมโครคอมพิวเตอร์ ซีพียู Intel Pentium III 950 MHz หน่วยความจำ 128 MB
ระบบปฏิบัติการ : Linux RedHat release 9.0, release name Shrike, kernel version 2.4.20-8



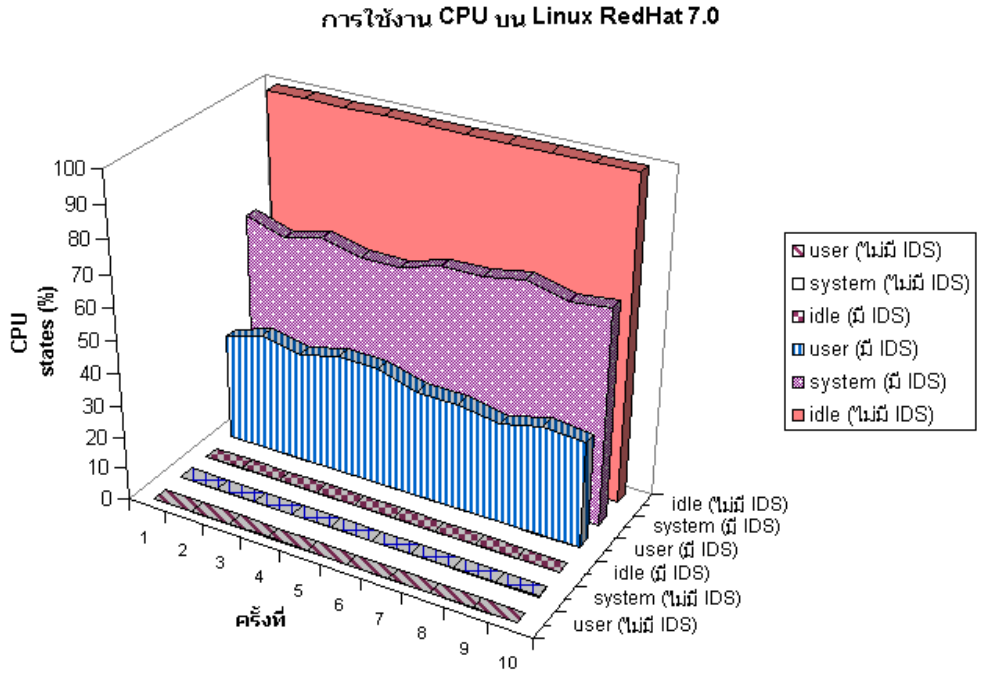
	1	2	3	4	5	6	7	8	9	10
user (ไม่มี IDS)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
system (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
idle (มี IDS)	0	0	0	0	0	0	0	0	0	0
user (มี IDS)	52.2	50.6	52	46.9	49.9	47.5	49.9	45	52	52.8
system (มี IDS)	47.7	49.3	47.9	53	50	51.2	50	54.9	47.9	47.1
idle (ไม่มี IDS)	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8

ภาพประกอบ 5.10 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1



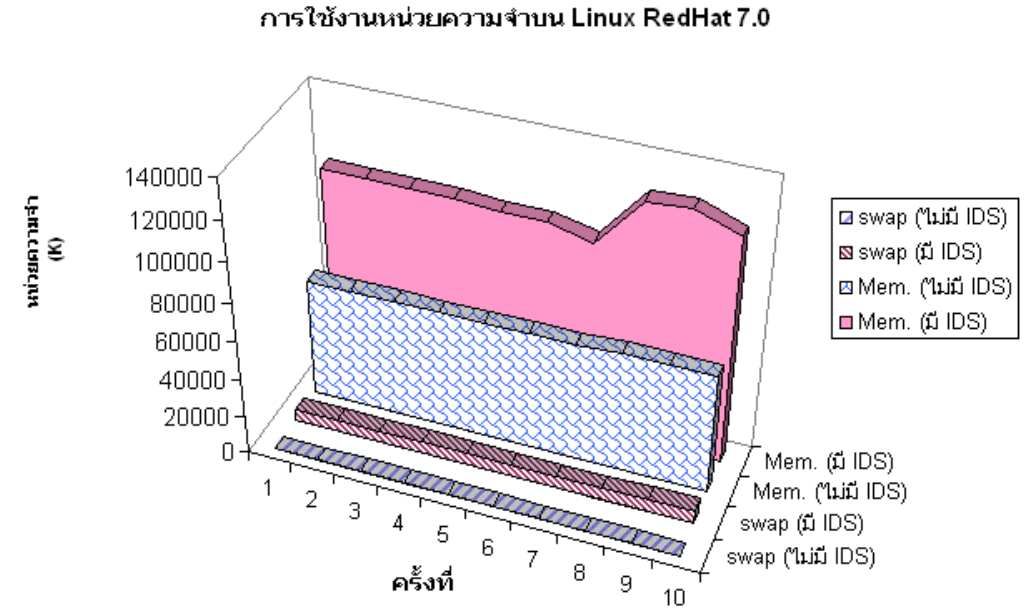
	1	2	3	4	5	6	7	8	9	10
swap (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
swap (มี IDS)	0	3,152	3,148	7,568	7,536	7,476	7,888	7,888	7,888	7,888
Mem. (ไม่มี IDS)	40,008	40,036	40,040	40,048	92,532	92,580	92,580	97,628	97,632	97,632
Mem. (มี IDS)	86,420	124,588	124,828	107,672	107,332	114,368	124,800	124,844	110,652	110,588

ภาพประกอบ 5.11 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1



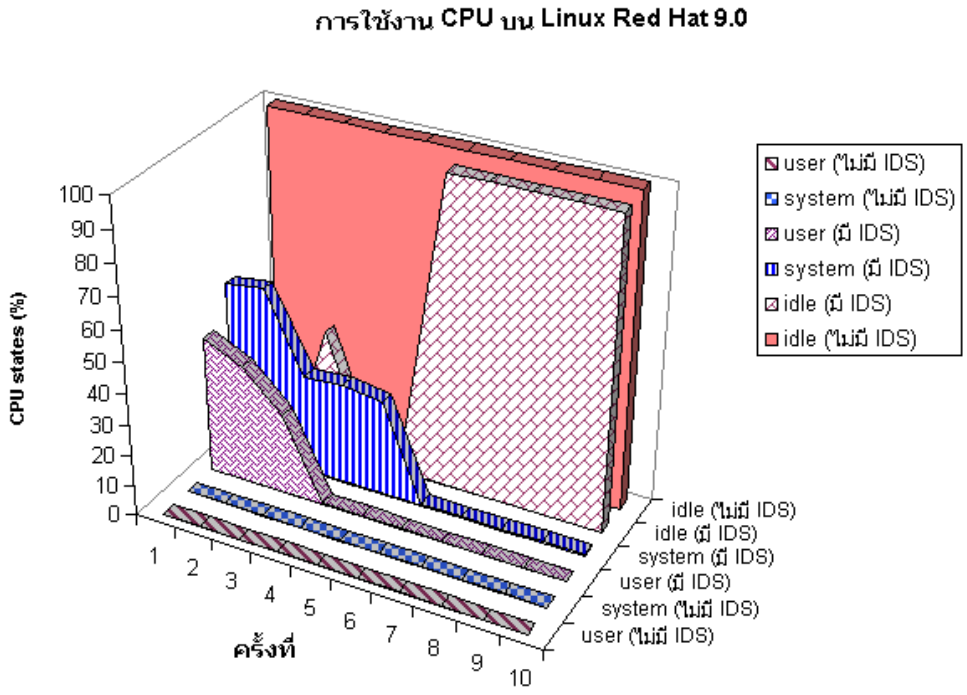
	1	2	3	4	5	6	7	8	9	10
user (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
system (ไม่มี IDS)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
idle (มี IDS)	0	0	0	0	0	0	0	0	0	0
user (มี IDS)	33.5	37.3	34.5	37.4	37.3	33.7	33.5	31.1	34.3	33
system (มี IDS)	66.4	62.6	65.4	62.5	62.6	66.2	66.4	68.8	65.6	66.9
idle (ไม่มี IDS)	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8	99.8

ภาพประกอบ 5.12 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0



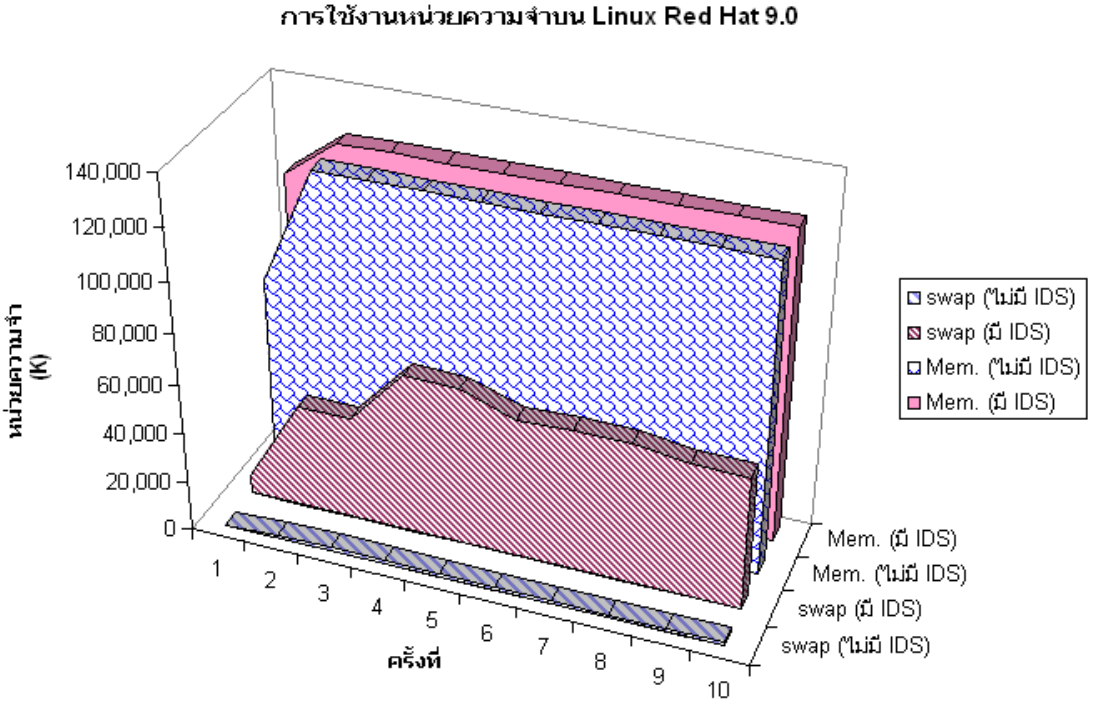
	1	2	3	4	5	6	7	8	9	10
swap (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
swap (มี IDS)	5,836	5,836	5,828	5,828	5,820	5,820	5,816	5,816	6,744	6,744
Mem. (ไม่มี IDS)	61,356	61,360	61,368	61,368	61,380	61,380	61,380	62,340	62,340	62,344
Mem. (มี IDS)	105,732	105,532	105,556	105,512	103,460	103,524	98,748	123,408	124,816	116,664

ภาพประกอบ 5.13 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0



	1	2	3	4	5	6	7	8	9	10
user (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
system (ไม่มี IDS)	0	0	0	0	0	0	0	0	0	0
user (มี IDS)	44.2	38.6	26.3	0.6	0.3	0.2	0.1	0.3	0	0.1
system (มี IDS)	55.7	57.2	32.1	32.8	31	0.8	0.7	0.7	0.9	0.7
idle (มี IDS)	0	0	40.1	4.1	9.6	98.9	99.1	98.9	99	99
idle (ไม่มี IDS)	100	100	100	100	100	100	100	100	100	100

ภาพประกอบ 5.14 กราฟแสดงการใช้งานซีพียูในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์ เรดแฮ็ท เวอร์ชัน 9.0



	1	2	3	4	5	6	7	8	9	10
swap (ไม่มี IDS)	0	1,068	1,076	1,076	1,076	1,092	1,092	1,092	1,084	1,652
swap (มี IDS)	7,496	41,452	41,804	64,012	63,484	56,092	57,024	56,976	53,884	53,548
Mem. (ไม่มี IDS)	76,696	123,588	123,588	123,596	123,596	123,332	123,332	123,340	123,076	122,872
Mem. (มี IDS)	108,088	123,584	123,804	123,736	123,804	123,776	123,804	123,800	123,804	123,804

ภาพประกอบ 5.15 กราฟแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่กับในขณะที่ไม่มีระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0

5.6 สรุป

เมื่อพิจารณากราฟแสดงความถูกต้องที่เปรียบเทียบการทำงานของระบบตรวจจับการบุกรุกก่อนและหลังปรับปรุงข้อมูลฝึกสอนระบบแยกตามเวอร์ชันของระบบปฏิบัติการลินุกซ์เรดแฮ็ทจะเห็นว่า เมื่อปรับปรุงการเก็บข้อมูลพฤติกรรมการทำงานของโปรเซสในแฟ้มข้อมูลฝึกสอนระบบแล้วระบบตรวจจับการบุกรุกจะทำงานตรวจสอบได้ดีขึ้นซึ่งจะเห็นได้จากค่าร้อยละของความถูกต้องในการตรวจสอบมีค่ามากขึ้นทั้งข้อมูลฝึกสอนระบบแบบเก่าและข้อมูลฝึกสอนระบบแบบใหม่ ดังในภาพประกอบ 5.3 และภาพประกอบ 5.4 สำหรับการทดสอบบนลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 ภาพประกอบ 5.8 สำหรับการทดสอบบนลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 และภาพประกอบ 5.9 สำหรับการทดสอบบนลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 การเปลี่ยนแปลงรูป-

แบบการเก็บข้อมูลในแฟ้มข้อมูลฝึกสอนระบบทำให้ความถูกต้องในการทำงานของระบบตรวจจับการบุกรุกเพิ่มมากขึ้นซึ่งแสดงไว้ในภาพประกอบ 5.5 ถึงภาพประกอบ 5.7

เมื่อพิจารณาการใช้งานซีพียูและหน่วยความจำบนระบบปฏิบัติการลินุกซ์เรดแฮ็ทจะเห็นว่า ในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่จะมีการใช้งานซีพียูและหน่วยความจำมากขึ้นดังที่ได้แสดงไว้ในตาราง 5.71 ถึงตาราง 5.73 จากภาพประกอบ 5.10 เมื่อระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 โปรเซสของผู้ใช้ (user) เข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 52.8% โปรเซสของระบบ (system) เข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 54.9% โดยที่ไม่มีการหยุดพัก (idle) เลย และเมื่อพิจารณาภาพประกอบ 5.11 ซึ่งแสดงการใช้งานหน่วยความจำในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 จะเห็นว่ามีการใช้งานหน่วยความจำแบบสับเปลี่ยน (swap memory) เพิ่มขึ้นประมาณ 2.98% และมีการใช้งานหน่วยความจำเพิ่มขึ้นประมาณ 21.28% บนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 7.0 สามารถพิจารณาการใช้งานซีพียูได้จากภาพประกอบ 5.12 จะเห็นว่าในขณะที่ระบบตรวจจับการบุกรุกทำงานอยู่โปรเซสของผู้ใช้เข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 37% โปรเซสของระบบเข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 68.8% โดยที่ไม่มีการหยุดพักเลย และจากภาพประกอบ 5.13 แสดงให้เห็นว่าเมื่อระบบตรวจจับการบุกรุกทำงานอยู่ มีการใช้งานหน่วยความจำแบบสับเปลี่ยนเพิ่มขึ้นประมาณ 2.54% และมีการใช้งานหน่วยความจำเพิ่มขึ้นประมาณ 48.9% และบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 9.0 เมื่อพิจารณาการใช้งานซีพียูจากภาพประกอบ 5.14 จะเห็นว่าเมื่อระบบตรวจจับการบุกรุกทำงานอยู่โปรเซสของผู้ใช้เข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 44.2% โปรเซสของระบบเข้าใช้งานซีพียูเพิ่มขึ้นประมาณ 57.2% มีช่วงการหยุดพักประมาณ 99% ลดลงจากปกติประมาณ 1% เมื่อพิจารณาการใช้งานหน่วยความจำจากภาพประกอบ 5.15 พบว่าเมื่อระบบตรวจจับการบุกรุกทำงานจะมีการใช้งานหน่วยความจำแบบสับเปลี่ยนเพิ่มขึ้นประมาณ 23.5% และมีการใช้งานหน่วยความจำเพิ่มขึ้นประมาณ 0.2%

โดยภาพรวมแล้วระบบตรวจจับการบุกรุกทำให้มีการใช้งานทรัพยากรของระบบมากขึ้น ในด้านของการตรวจจับการบุกรุก ระบบตรวจจับการบุกรุกมีความสามารถในการตรวจจับเป็นที่น่าพอใจเนื่องจากเกิดความผิดพลาดในการตรวจจับเพียงเล็กน้อย ในบทถัดไปจะเป็นการอภิปรายและสรุปผลเกี่ยวกับระบบตรวจจับการบุกรุกที่นำเสนอนี้