# Linux command ในการค้นหาไฟล์ที่ถูกบุกรุกด้วย (grep)

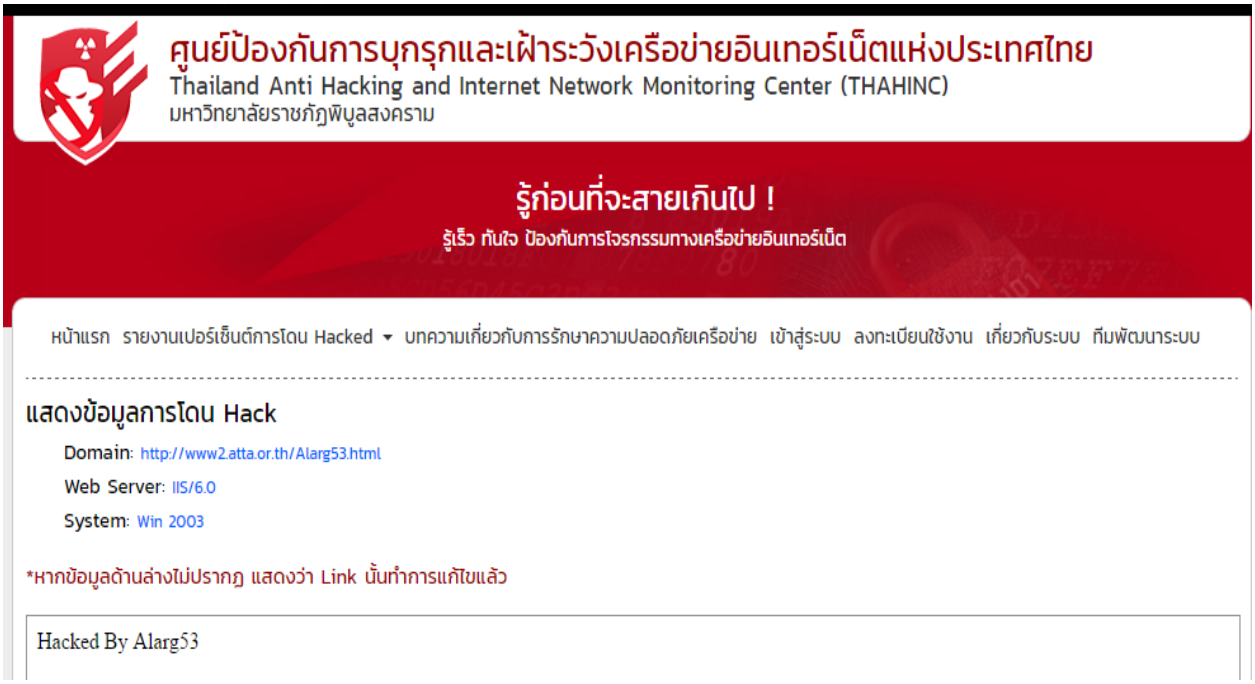
**ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช** : เขียน

Asst. Prof. Dr. Kittipong Suwannaraj

ECA , MTCNA, MTCUME, MTCTCE, RHCT

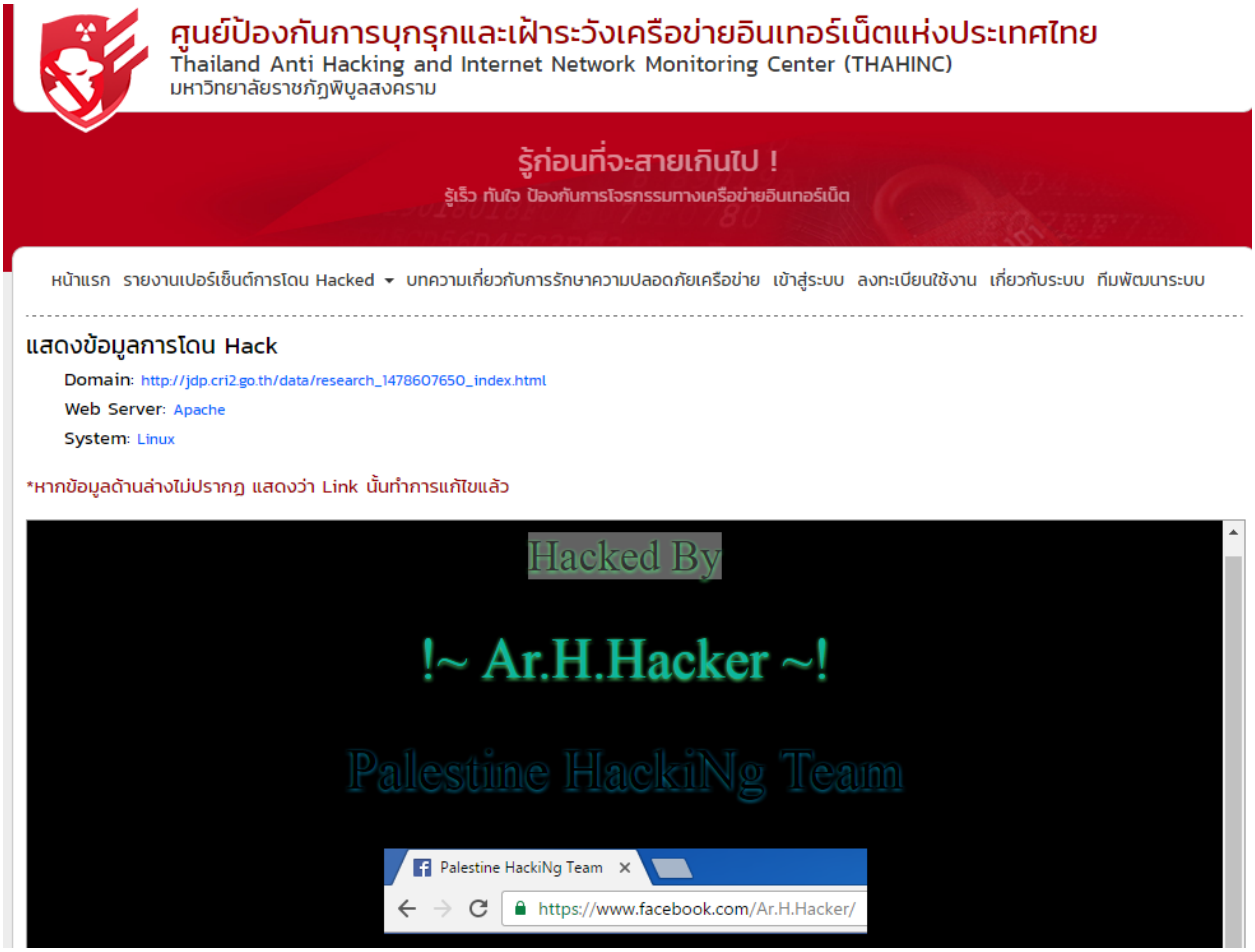
kitti@psru.ac.th

วันนี้ขอนำเสนอบทความเกี่ยวกับการใช้คำสั่งของ Linux หรือ Unix ในการค้นหาไฟล์ที่ Hacker ได้สร้างไว้เมื่อบุกรุกเครือข่ายสำเร็จ โดยปกติแล้วเมื่อ Hacker ทำการบุกรุกแล้วจะสร้างไฟล์ข้อความ (Text file) ไว้โดยภายในนั้น ส่วนใหญ่จะมีคำว่า “Hacked” หรืออาจจะเป็นคำว่า “Hacked by” แล้วตามด้วยข้อความอื่นๆ ที่เขาอยากจะพิมพ์ลงไป ดังตัวอย่างของหน้าจอที่ได้ยกตัวอย่างให้ดูดังภาพ




รูปที่ 1 ตัวอย่างของหน้าจอเมื่อ Hacker บุกรุกเครื่องแม่ข่ายสำเร็จ 1

## Linux command ในการค้นหาไฟล์ที่ถูกบุกรุกด้วย (grep)




รูปที่ 2 ตัวอย่างของหน้าจอเมื่อ Hacker บุกรุกเครื่องแม่ข่ายสำเร็จ 2

จากข้อมูลที่ได้คือ ข้อความคำว่า “Hacked” จะถูกนำมาใช้งานบ่อยมาก ซึ่งเราสามารถนำเอาคำนี้ มาเป็น Keyword ในการค้นหาไฟล์ข้อความต่าง ๆ ที่เก็บไว้บน Web Server ของเราได้โดยใช้คำสั่งของ Linux ที่ชื่อว่า grep ในการค้นหาคำ ๆ นี้ได้ ยกตัวอย่างเช่น

```
#  grep –rl “Hacked”  /var/www/html
        /var/www/html/b.html                (ผลลัพธ์เมื่อค้นเจอคำว่า “Hacked” ในไฟล์ b.html
```

จากตัวอย่างด้านบนนี้ เราใช้คำส่ง grep ในการค้นหาคำว่า “Hacked” ทุกไฟล์ที่เก็บไว้ใน /var/www/html โดย

-r หมายถึง ค้นหาใน Sub directory ที่อยู่รองลงมาด้วย

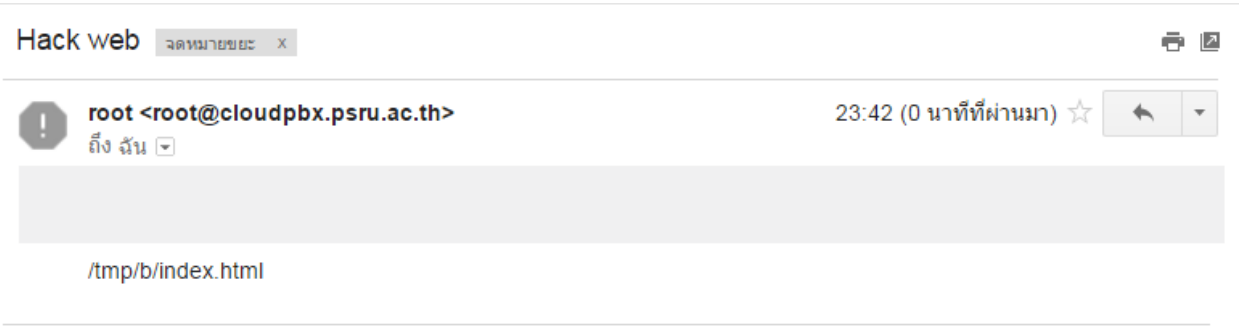
-l หมายถึง คำค้นหานั้นจะต้องเหมือนกันเท่านั้น

## Linux command ในการค้นหาไฟล์ที่ถูกบุกรุกด้วย (grep)

ตัวอย่างต่อมา เราจะใช้คำสั่ง grep ในการค้นหาเหมือนกับคำสั่งก่อนหน้านี้ แล้วเราจะให้ระบบส่งอีเมล (email) ไปหาเมลที่เราต้องการด้วยเราสามารถสั่งงานได้ดังนี้

```
# grep –rl “hacked” /var/www/html | mail –s “Hacked web” kitti@psru.ac.th
```

เมื่อทำการรันคำสั่งนี้แล้ว ระบบจะทำการค้นหาไฟล์ที่ถูกบุกรุก เมื่อได้ผลลัพธ์มาก็จะทำการส่งอีเมล์ไปยัง kitti@psru.ac.th โดยใช้หัวข้อว่า “Hacked web” ดังรูป




รูปที่ 3 อีเมล์ส่งมาแจ้งเตือนว่ามีได้ค้นพบว่าไฟล์ index.html มีคำว่า “hacked” อยู่ภายในนั้น

เมื่อได้รับทราบถึงการตรวจสอบไฟล์ข้อความที่ Hacker สร้างหรือนำมาวางไว้บนเครื่อง Web Server ของเราแล้ว ก็สามารถหาทางแก้ไข หรือทำให้ระบบแจ้งเตือนเราแบบอัตโนมัติก็ได้ โดยการประยุกต์กับคำสั่ง crontab เข้ามาช่วย เช่น บอกให้ crontab รันคำสั่ง grep ทุก 06.00 น. ทุกวัน แล้วแจ้งเตือนเราผ่านทางอีเมลเป็นต้น

**แหล่งสืบค้นข้อมูล :**

http://askubuntu.com/questions/55325/how-to-use-grep-command-to-find-text-including-subdirectories

**Article number** : 201609111600