# Hack window with LLMNR/NBNS Poisoning

## หลักการและเหตุผล

การใช้งานอินเตอร์เน็ตมีความเสี่ยงที่จะโดน hack ข้อมูล ต่าง ๆ ที่เราใช้งานอยู่ ทั้งข้อมูลส่วนตัว ข้อมูลในคอมพิวเตอร์ และจะมีวิธีป้องกันอย่างไร ? เราเห็นถึงอันตรายในการใช้งานอินเตอร์เน็ต จึงทำเพื่อสาธิตและแสดงให้เห็นถึงความอันตรายจากการใช้อินเตอร์เน็ตโดยไม่คำนึงถึงความปลอดภัย

## วัตถุประสงค์

1.เพื่อศึกษากลไกการทำงานของโปรแกรมและวิธีโจรกรรมข้อมูลทางคอมพิวเตอร์
2.เพื่อพัฒนาและศึกษาการป้องกันจากการโจมตี
3.ติดตั้งและปรับแต่ง

## ความสามารถ

ดักเอา username password ต่างๆที่ผู้ใช้งานกรอกเพื่อเข้าถึงพาร์ทโฟล์เดอร์ในเครื่องและเพื่อเข้าใช้งานเว็บบราวเซอร์ที่ไม่มีอยู่จริงได้

## เครื่องมือที่เกี่ยวข้อง

-Kali Linux
-vmware workstation pro 16

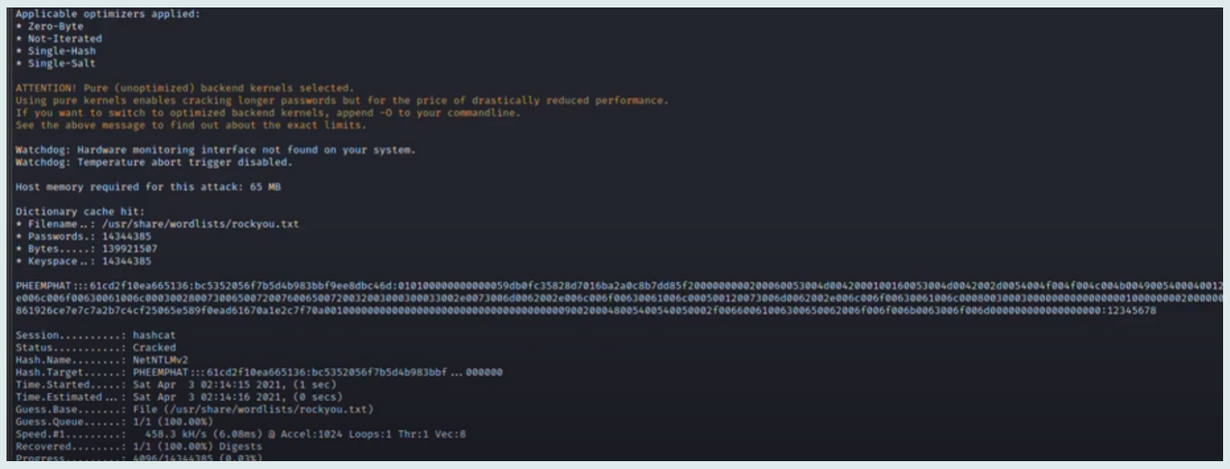
## ขั้นตอนการทำงาน

1.เปิดโปรแกรม Kali Linux โดยแฮกเกอร์กับเหยื่ออยู่ใน local subnetwork วงเดียวกัน

2.Hackerก็ทำการเปิดโปรแกรม Responder ระบุ network interface ระบุ IPaddress ของตัวเอง

3.เครื่องเหยื่อ #1 เป็น Windows 7 อยู่ที่ IP address 192.168.15.149 ก็ได้พยายามเข้าเซิร์ฟเวอร์ไฟล์ที่ พิมพ์ผิดหรือไม่มีอยู่จริงในกรณีนี้คือ \\sthfileshare\secret จากนั้นเครื่องเหยื่อ #2 เป็น Windows 10 อยู่ที่ IP address 192.168.15.153 ก็ได้พยายามเข้าเว็บ sthbanking.com ด้วย Google Chrome แต่ดันพิมพ์ผิดลืมใส่จุด ไปเข้าเว็บ sthbankingcom แทน

4.จากนั้นแฮกเกอร์ก็นำค่า Net-NTLMv2 ที่ได้มาจากเหยื่อทั้งสองคนมาเก็บใส่ในไฟล์ชื่อ ntlmv2-demo.txt แล้วก็ทำการลอง แครก ด้วยโปรแกรม hashcat ใช้เวลาแค่ 7 วินาที แฮกเกอร์ก็สามารถแกะรหัสผ่านของเหยื่อทั้งสองคนออกมาได้




## จัดทำโดย
## Group 1 Section 1

นายกิติศักดิ์ อนุสิทธิ์ 623020366-4
นายทักษิณ คะสาราช 623020369-8
นางสาวนันทพร เจริญยิ่ง 623020376-1
นายภีมภัทร์ ภูไทกัมปนาทภิญญา 623020688-2
นายเวคิน สอนเวียง 623020691-3
นางสาวศุภางค์ สุวรรณโคตร 623020966-0