
รายงาน

# Kerberos

จัดทำโดย

นางสาวชาลิสา กลัดแพ รหัสนักศึกษา 6130200251

นางสาวณัฐนิชา ชูศิลป์ รหัสนักศึกษา 6130200358

นางสาวปานวาด ปัดทุมแฝง รหัสนักศึกษา 6130200617

คณะวิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์ (S05)

เสนอ

อาจารย์จาอุดมพร ตุงคะศิริ

รายงานนี้เป็นส่วนหนึ่งของรายวิชา Information Systems Security (01418332)

ภาคเรียนที่ 2 ปีการศึกษา 2563

มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตศรีราช

# คำนำ

รายงานฉบับนี้เป็นส่วนหนึ่งของรายวิชา Information Systems Security (01418321)โดยมีจุดประสงค์เพื่อการศึกษาเกี่ยวกับ Kerberos , องค์ประกอบของ Kerberos และการทำงานของ Kerberos คณะผู้จัดทำขอขอบคุณ อาจารย์อุดมพร ตุงคะศิริ ผู้ให้ความรู้และแนวทางการศึกษา รวมถึงเพื่อน ๆ ทุกคนที่ให้ความช่วยเหลือมาโดยตลอด คณะผู้จัดทำหวังว่ารายงานฉบับนี้จะให้ความรู้ และเป็นประโยชน์แก่ผู้อ่านทุก ๆ ท่าน

คณะผู้จัดทำ

12 กุมภาพันธ์ 2564

# สารบัญ

# Kerberos

**Kerberos**

Kerberosออกแบบและพัฒนาโดย Needham และ Schroeder จาก Massachusetts Institute of Technology (MIT)เป็น Protocolสำหรับใช้พิสูจน์ความเป็นตัวตนผ่านเครือข่ายแบบ Single Sign-On (พิสูจน์ตัวตนเพียงครั้งเดียวแต่สามารถเข้าใช้บริการของ Serverได้มากกว่าหนึ่งบริการ) โดยหลักการในภาพรวมคือผู้ใช้งานจะไปขอตั๋ว (Kerberos ticket) มาจากเซิร์ฟเวอร์ที่ทำหน้าที่เป็น Kerberos Distribution Center (KDC) จากนั้นเอาตั๋วนั้นไปโชว์ให้เครื่องปลายทางที่เราจะล็อกอิน เพื่อการเข้าไปใช้

**Kerberos**

-เป็นสถาปัตยกรรมแบบ Client/Server

-ที่ใช้การเข้ารหัสแบบ Symmetric (Secret Key) Cryptography

-จะมีการสร้าง Login Session เมื่อป้อน Username และ Password ถูกต้อง

-ในระหว่างการใช้งาน Resource ของ Server จะมีการตรวจสอบ Session เป็นระยะ ๆ เนื่องจาก Login Session มีอายุการใช้งาน

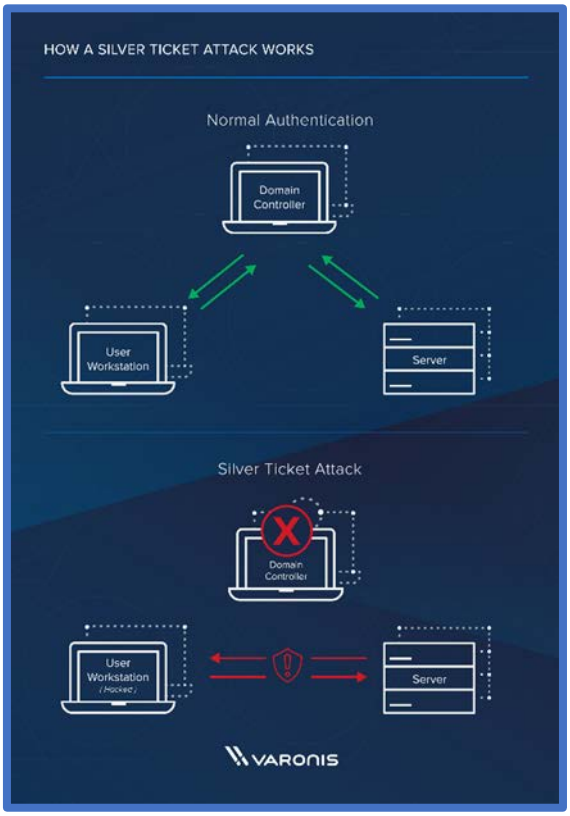
**ในการเข้าใช้ Kerberos**

ครั้งแรกผู้ใช้ต้องทำการร้องขอ Ticket ผ่านโปรแกรม kinit โดย Principal (ชื่อบัญชีผู้ใช้หรือชื่อบริการสำหรับใช้ในการพิสูจน์ตัวตน) ของผู้ใช้จะถูกส่งไปยัง Kerberos Server ซึ่งภายในประกอบด้วย Authentication Service (AS) และ Ticket Granting Service (TGS)

**การโจมตีที่อาจเกิดขึ้นได้กับ Kerberos**

-Silver Tickets เป็น Ticket Granting Service (TGS) ซึ่งเป็น service tickets สามารถสร้างได้โดย crack account password ในเครื่อง user แล้วนำมาสร้าง fake authentication ticket ซึ่ง Kerberos อนุญาตให้ใช้ services login เข้าสู่ระบบโดยไม่มีการ check ว่า token นั้น valid หรือไม่ โดย ticket ดังกล่าวทำให้เราสามารถเข้าถึง service บาง service ที่ใช้ Kerberos เป็นส่วน authenticate

- Golden Tickets KRBTGT account ซึ่งใช้ในการ encrypt และ sign Kerberos ticket ทั้งหมด โดย Account นี้ password จะไม่มีหมดอายุ และ KRBTGT จะไม่มีการเปลี่ยนชื่อใน domain ใดๆ จะเหมือนเดิมตลอด สิ่งที่ต้องทำให้ได้คือเอา KRBTGT password hash มาให้ได้ก่อน ซึ่งเป็นส่วนสำคัญสุด โดยการจะได้มาซึ่ง password hash นั้นเราต้องเข้าถึง AD และใช้สิทธิ์ admin ให้ได้ก่อน



**ระบบ Kerberos**

ประกอบขึ้นจากสองส่วนหลักคือ

1.Ticket ใช้สำหรับการพิสูจน์ตัวตนของผู้ใช้ในระบบ และการเข้ารหัสข้อมูล

2.Authenticator ใช้ในการตรวจสอบ Ticket ว่าเป็นผู้ใช้คนเดียวกันที่ใช้ Ticket เป็นใบเบิกทางเข้าสู่ระบบ และเป็นผู้ใช้ที่ระบบสร้างให้อย่างถูกต้อง

**Kerberos เซิร์ฟเวอร์ มีสองส่วนบริการในการใช้งานคือ**

1.Authentication service (AS) สำหรับการพิสูจน์ตัวตนของผู้ใช้กับ Kerberos เซิร์ฟเวอร์ก่อนการเข้าใช้บริการ

2.Ticket Granting Service (TGS) เป็นบริการที่ออก Ticket เพื่อให้ผู้ใช้นำไปใช้กับเซิร์ฟเวอร์ที่ต้องการ

**กระบวนการใช้งานระบบ Kerberos มีลำดับดังนี้**

1.ผู้ใช้จะทำการพิสูจน์ตัวตนครั้งแรกกับ Authentication service ของ Kerberos ซึ่งจะได้กุญแจสมมาตรซึ่งจะใช้ในการเข้ารหัสข้อมูลในการติดต่อสื่อสาร

2.ก่อนผู้ใช้จะเข้าไปใช้บริการใด ๆ ในระบบได้ต้องมี Ticket ก่อน ด้วยการติดต่อไปที่ Ticket Granting Service เพื่อให้ออก Ticket ที่เหมาะสมกับการเข้าไปใช้บริการบนเซิร์ฟเวอร์ในระบบได้

3.ผู้ใช้นำ Ticket สำหรับไปใช้กับการร้องขอการติดต่อการบริการจากเซิร์ฟเวอร์ในระบบ

**ปัญหาสำคัญ**

ของการใช้ระบบ Kerberos คือการขยายระบบเนื่องจากเซิร์ฟเวอร์ Kerberos ต้องเก็บกุญแจของผู้ใช้ทุกคนที่เข้ามาในระบบ ถ้าระบบใหญ่มากขึ้น มีการกระจายตัวมากกว่าหนึ่งจุด ย่อมส่งผลเสียต่อการใช้งานระบบโดยรวม แต่การนำระบบ Kerberos มาใช้จะเพิ่มความสะดวกในการพิสูจน์ตัวตนได้มากขึ้น มักเรียกการใช้งาน Kerberos ว่าเป็นระบบ Single Sign-On แบบหนึ่ง คือการเข้าถึงการใช้บริการของระบบทั้งหมดได้ด้วยการพิสูจน์ตัวตนยงครั้งเดียว

**การทำงานของ Kerberos**

Kerberos จะต้องมีส่วนของเซิร์ฟเวอร์เอาไว้ยืนยันตัวตนชื่อว่า Key Distribution Center (KDC) ซึ่งประกอบไปด้วย 2 ส่วนย่อยคือ Authentication Server (AS) กับ Ticket Granting Server (TGS) มีขั้นตอนดังนี้

1. ขั้นตอน AS-REQ Client Computer จะส่งชื่อ Username ที่จะล็อกอินไปหา KDC (AS) เพื่อขอตั๋ว

2. ขั้นตอน AS-REP KDC (AS) จะตอบกลับมา 2 อย่างคือ

- ตั๋วเอาไว้ยืนยันคนที่ขอล็อกอินเรียกว่า Ticket Granting Ticket (TGT) ซึ่งตั๋วนี้จะถูกเข้ารหัสไว้ โดยที่คนขอจะถอดรหัสไม่ได้ (และไม่จำเป็นจะต้องถอดรหัส TGT) แต่เอาไปใช้ต่อที่ TGS ได้ ถ้ามี session key
- ข้อมูลเพิ่มเติมอีกส่วน ที่ถูกเข้ารหัสด้วยรหัสผ่านของ domain user account ที่ขอไป (longcat) ซึ่งจะมีค่ากุญแจชั่วคราว (session key) และอื่น ๆ

3. ขั้นตอน TGS-REQ Client Computer พอได้ตั๋ว TGT พร้อมกับ session key ก็จะเอาไปคุยกับ KDC อีกรอบ แต่คราวนี้จะคุยกับส่วน TGS เพื่อขออีกตั๋วเรียกว่า service ticket เพื่อเข้าไปใช้งานระบบอื่น

4. ขั้นตอน TGS-REP ซึ่ง TGS ก็จะตอบกลับเพื่อให้ service ticket ใครก็ตามที่เอา TGT กับ session key มาขอเสมอ (แต่จะเอา service ticket ไปแล้วใช้ได้หรือเปล่าไม่อาจทราบได้) โดยใน service ticket ก็จะมีระบุว่าคนที่ขอไปเป็นใคร ขอเมื่อไร

5. ขั้นตอน AP-REQ ต่อมา Client Computer ก็จะส่ง service ticket ไปยังเซิร์ฟเวอร์ที่ตัวเองต้องการจะเชื่อมต่อ เพื่อขอเข้าไปใช้งานระบบ โดย service ticket จะโดนเข้ารหัสอยู่ ซึ่งจะมี service account (คือ domain user ที่สร้างมาไว้สำหรับเข้าไปใช้งาน service เท่านั้น) ของเซิร์ฟเวอร์คนเดียวที่จะถอดรหัสได้ พอเซิร์ฟเวอร์ได้รับ service ticket ก็จะตรวจสอบดูข้างในว่า Client Computer เป็นใคร ควรเข้าระบบตัวเองได้หรือเปล่า

6. ขั้นตอน AP-REP เซิร์ฟเวอร์หลังตรวจสอบว่าคนขอเป็นใคร มีสิทธิ์เข้าระบบหรือเปล่า ก็จะตอบกลับไปว่ายอมให้ Client Computer เข้าระบบไหม หรือเริ่มการเชื่อมต่อหลังเข้าสู่ระบบได้ทันทีเลย

# อ้างอิง

https://wordpress.com/?ref=footer_blog (เข้าถึงวันที่12/2/64)

https://www.techsuii.com/2017/09/04/summary-kerberos-authentication-protocol/ (เข้าถึงวันที่12/2/64)

https://www.catcyfence.com/it-security/article/kerberos-authentication-vulnerabilities/

(เข้าถึงวันที่11/2/64)

https://www.google.com/search?safe=active&ei=gf0kYPm7O4rVz7sPoMqmEA&q=kerberos+%E0%B8%84%E0%B8%B7%E0%B8%AD&oq=kerberos+%E0%B8%84%E0%B8%B7%E0%B8%AD&gs_lcp=CgZwc3ktYWIQAzIECAAQEzIECAAQEzIICAAQFhAeEBMyCAgAEBYQHhATMggIABAWEB4QEzIICAAQFhAeEBM6BwgAELADEM6BAgAEEM6AggAOgYIABAWEB46BQghEKABUIFCWP5rYPNtaARwAngAgAGpAYgB2QiSAQMwLjiYAQCgAQGqAQdnd3Mtd2l6yAEKwAEB&sclient=psy-ab&ved=0ahUKEwi5gOLpxuHuAhWK6nMBHSClCQIQ4dUDCA0&uact=5# (เข้าถึงวันที่11/2/64)