



# **Securing Microsoft Windows**

ST2612

Written by: Lee Yi Terng (1904189)

DISM/FT/2A/04

Submitted To: Ms Teo Soek Ling

Date: 22th August 2020

# Questions

## 1. Which Institute/Organization invented Kerberos?

Ans: Massachusetts Institute of Technology

## 2. List all the possible types of 'tickets' that Kerberos can be issued.

Ans: Service and Authentication

## 3. Identify the TWO possible events that can trigger the Kerberos server to issue out a new "ticket-granting ticket"?

Ans: If you are accessing a network resource. If you are accessing another system in a domain.

## 4. Please take one or a couple of screenshots while you are using the klist command to show at least 3 cached tickets (any types) you have obtained from your own SMW Domain Kerberos server. Attach your screenshot(s) that show the commands and output as part of the solution submission. (Screen captured images downloaded from the internet are not counted).

Ans:

```
C:\Windows\system32>klist | more

Current LogonId is 0:0x7c14f

Cached Tickets: (3)

#0>    Client: smw_srv2016 @ SMW.ASSIGNMENT.COM
      Server: krbtgt/SMW.ASSIGNMENT.COM @ SMW.ASSIGNMENT.COM
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
      Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
      Start Time: 8/14/2020 11:58:20 (local)
      End Time:   8/14/2020 21:58:20 (local)
      Renew Time: 8/21/2020 11:53:31 (local)
      Session Key Type: AES-256-CTS-HMAC-SHA1-96
      Cache Flags: 0x1 -> PRIMARY
      Kdc Called: SERVER1

#1>    Client: smw_srv2016 @ SMW.ASSIGNMENT.COM
      Server: host/SERVER1 @ SMW.ASSIGNMENT.COM
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
      Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
      Start Time: 8/14/2020 11:58:20 (local)
      End Time:   8/14/2020 21:58:20 (local)
      Renew Time: 8/21/2020 11:53:31 (local)
      Session Key Type: AES-256-CTS-HMAC-SHA1-96
      Cache Flags: 0
      Kdc Called: SERVER1

#2>    Client: smw_srv2016 @ SMW.ASSIGNMENT.COM
      Server: cifs/SERVER2 @ SMW.ASSIGNMENT.COM
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
      Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
      Start Time: 8/14/2020 11:56:03 (local)
      End Time:   8/14/2020 21:53:31 (local)
      Renew Time: 8/21/2020 11:53:31 (local)
      Session Key Type: AES-256-CTS-HMAC-SHA1-96
      Cache Flags: 0
      Kdc Called: SERVER1

C:\Windows\system32>
```