Forged Kerberos Ticket Indicators
Detecting Golden & Silver Ticket Use

Sean Metcalf (sean [@] dansolutions.com)

SILVER TICKETS

Normal, valid account logon event data structure:
Security ID: DOMAIN\AccountID
Account Name: AccountID
Account Domain: DOMAIN

Silver Ticket events may have one of these issues:

- The Account Domain field is blank when it should be DOMAIN
- The Account Domain field is DOMAIN FQDN when it should be DOMAIN.

Event ID: 4624 (Account Logon)
Account Domain is FQDN & should be short domain name
Account Domain: LAB.ADSECURITY.ORG [ADSECLAB]

Event ID: 4634 (Account Logoff)
Account Domain is blank & should be short domain name
Account Domain: _____ [ADSECLAB]

Event ID: 4672 (Admin Logon)
Account Domain is blank & should be short domain name
Account Domain: _____ [ADSECLAB]

GOLDEN TICKETS

Normal, valid account logon event data structure:
Security ID: DOMAIN\AccountID
Account Name: AccountID
Account Domain: DOMAIN

Golden Ticket events may have one of these issues:

- The Account Domain field is blank when it should be DOMAIN
- The Account Domain field is DOMAIN FQDN when it should be DOMAIN.

Event ID: 4624 (Account Logon)
Account Domain is FQDN & should be short domain name
Account Domain: LAB.ADSECURITY.ORG [ADSECLAB]

Event ID: 4672 (Admin Logon)
Account Domain is blank & should be short domain name
Account Domain: _____ [ADSECLAB]

MS14-068 Exploit Tickets

Normal, valid account logon event data structure:
Security ID: DOMAIN\AccountID
Account Name: AccountID
Account Domain: DOMAIN

MS14-068 events may have one of these issues:

- The Account Domain field is blank when it should be DOMAIN
- The Account Domain field is DOMAIN FQDN when it should be DOMAIN.
- Account Name is a different account from the Security ID.

PYKEK

Event ID: 4624 (Account Logon)
The Account Domain field is DOMAIN FQDN when it should be DOMAIN.
Account Name is a different account from the Security ID

Event ID: 4672 (Admin Logon)
The Account Domain field is DOMAIN FQDN when it should be DOMAIN.
Account Name is a different account from the Security ID

Event ID: 4768 (Kerberos TGS Request)
The Account Domain field is DOMAIN FQDN when it should be DOMAIN.

KEKEO

Event ID: 4624 (Account Logon)
The Account Domain field is DOMAIN FQDN when it should be DOMAIN.

Event ID: 4672 (Admin Logon)
Account Domain is blank & should be DOMAIN.

Event ID: 4768 (Kerberos TGS Request)
The Account Domain field is DOMAIN FQDN when it should be DOMAIN.