Comprehensive, Multi-Source Cyber-Security Events

Analysis of Windows-Based Authentication Events

Los Alamos National Laboratory's Corporate, Internal Computer Network

Damita J. Zweiback

Binary Classifier for Authentication

	Successful Log-On	**Failed Log-On**
Trusted Source	C1 = True-Verified Authentication	C2 = False-Unverified Authentication
Untrusted Source	C4 = False-Verified Authentication	C3 = True-Unverified Authentication

Analysis

- The auth.csv file was examined and filtered to study the patterns of data in each field.
- First, the “Fail” and “Success” results were examined separately and filtered on the “LogOn” value of the Authentication Orientation column.
- Second, the Authentication Type and LogOn Type values were filtered and examined for patterns.
- Finally, a review of the source user@domain **(su)**, destination user@domain**(du)**, source computer **(sc)** and destination computer **(dc)** were examined for additional patterns.
- The data was coded as follows:

	Successful Log-On	**Failed Log-On**
Trusted Source	If **su** = **du** AND **sc** OR **dc** shared the same value as **su** and **du** code as C1 (e.g. 4/4 or 3/4 of the numerical values matched) **C1 = True-Verified Authentication**	If **su** = **du** AND **sc** OR **dc** shared the same value as **su** and **du** code as C2 (e.g. 4/4 or 3/4 of the numerical values matched) **C2 = False-Unverified Authentication**
Untrusted Source	If **su** OR **du** shared the same numerical value as **sc** OR **dc** code as C4 (e.g. 2/4 or 1/4 of the numerical values matched) **C4 = False-Verified Authentication**	If **su** OR **du** shared the same numerical value as **sc** OR **dc** code as C3 (e.g. 2/4 or 1/4 of the numerical values matched) **C3 = True-Unverified Authentication**

Evaluation of Data

	Successful Log-On	**Failed Log-On**	
Trusted Source	(.9982) C1 = True-Verified Authentication 420,033 events **(.9668)**	(.0017) C2 = False-Unverified Authentication 725 events **(.4453)**	(.99)
Untrusted Source	(.9411) C4 = False-Verified Authentication 14,430 events **(.0332)**	(.0589) C3 = True-Unverified Authentication 903 events **(.5547)**	(1.00)
	434,463	1,628	
	(1.00)	(1.00)	

Conclusion

- The results of the evaluation indicate that the majority of events were true-verified successful LogOns (.97); e.g. the user was a trusted source and verification was authentic.

- Three percent (.03) of successful LogOns were identified as false-verified events; e.g. the user was an untrusted source and verification was authenticated.

- Of the failed LogOns, a little less than half (.45) were false-unverified events; e.g. the user was a trusted source, but authentication could not be verified.

- Fifty-five percent (.55) of the failed LogOns were coded as true-unverified events; e.g. the user was an untrusted source and authentication could not be verified.

Additional Analysis:

- The next steps of this analysis are to write a program code (using machine language and a statistical procedure such as logistic regression or K-means clustering to group and test the predictability of the patterns identified.

- The next slide shows a partial start of the code written in Jupyter notebook.

This NextRev exercise examines the output of the auth.txt.gz file and creates and evaluates a binary classification.

In [9]:
```
# Dependencies and Setup
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt

# File to Load
file_to_load = "Resources/auth.csv"

# Read auth file and store into Pandas data frome
auth_data = pd.read_csv(file_to_load)

# Show data
auth_data.head(10)
```

Out[9]:

	1	ANONYMOUS LOGON@C586	ANONYMOUS LOGON@C586.1	C1250	C586	NTLM	Network	LogOn	Success
0	1	ANONYMOUS LOGON@C586	ANONYMOUS LOGON@C586	C586	C586	?	Network	LogOff	Success
1	1	C101$@DOM1	C101$@DOM1	C988	C988	?	Network	LogOff	Success
2	1	C1020$@DOM1	SYSTEM@C1020	C1020	C1020	Negotiate	Service	LogOn	Success
3	1	C1021$@DOM1	C1021$@DOM1	C1021	C625	Kerberos	Network	LogOn	Success
4	1	C1035$@DOM1	C1035$@DOM1	C1035	C586	Kerberos	Network	LogOn	Success
5	1	C1035$@DOM1	C1035$@DOM1	C586	C586	?	Network	LogOff	Success