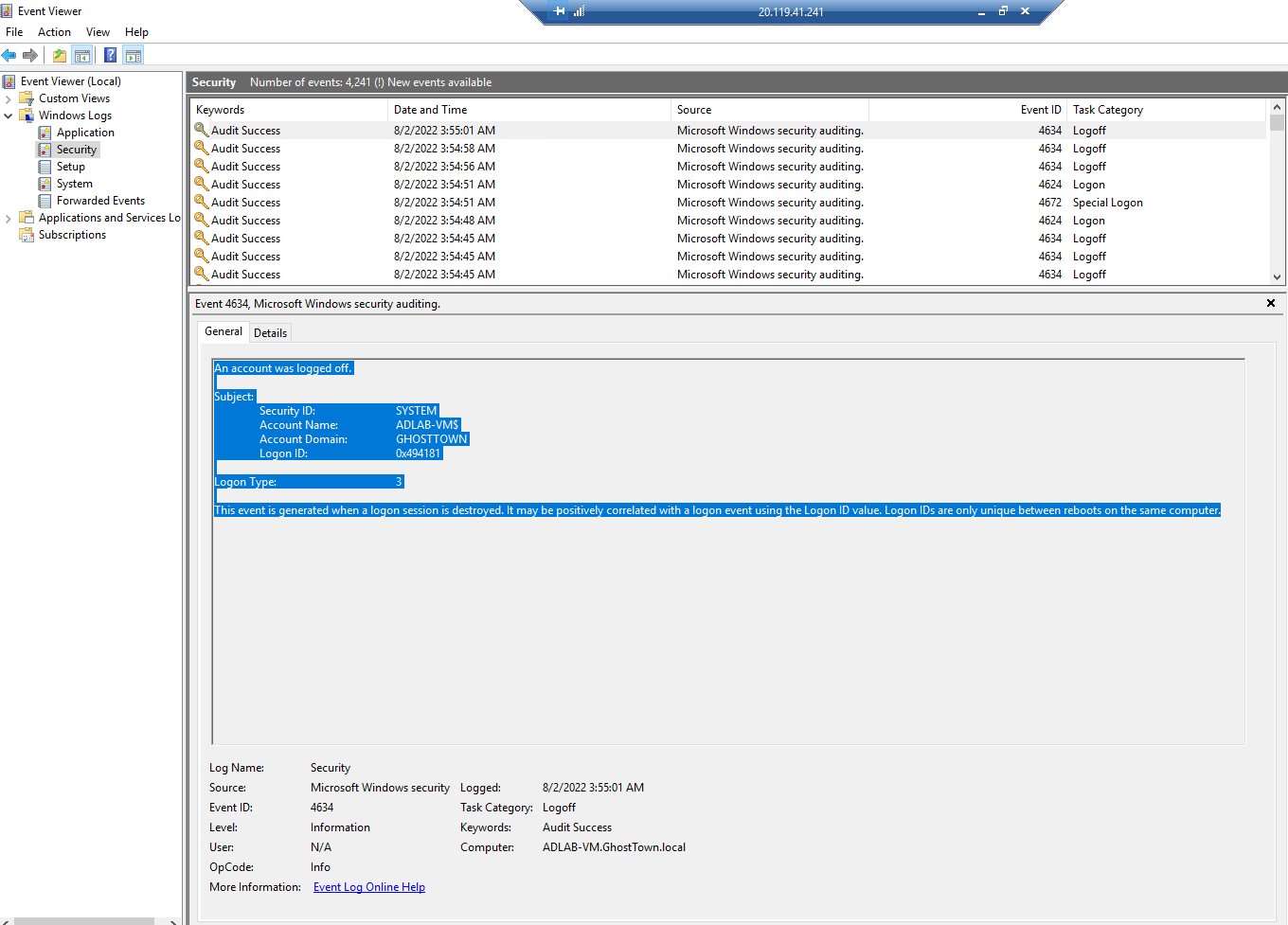
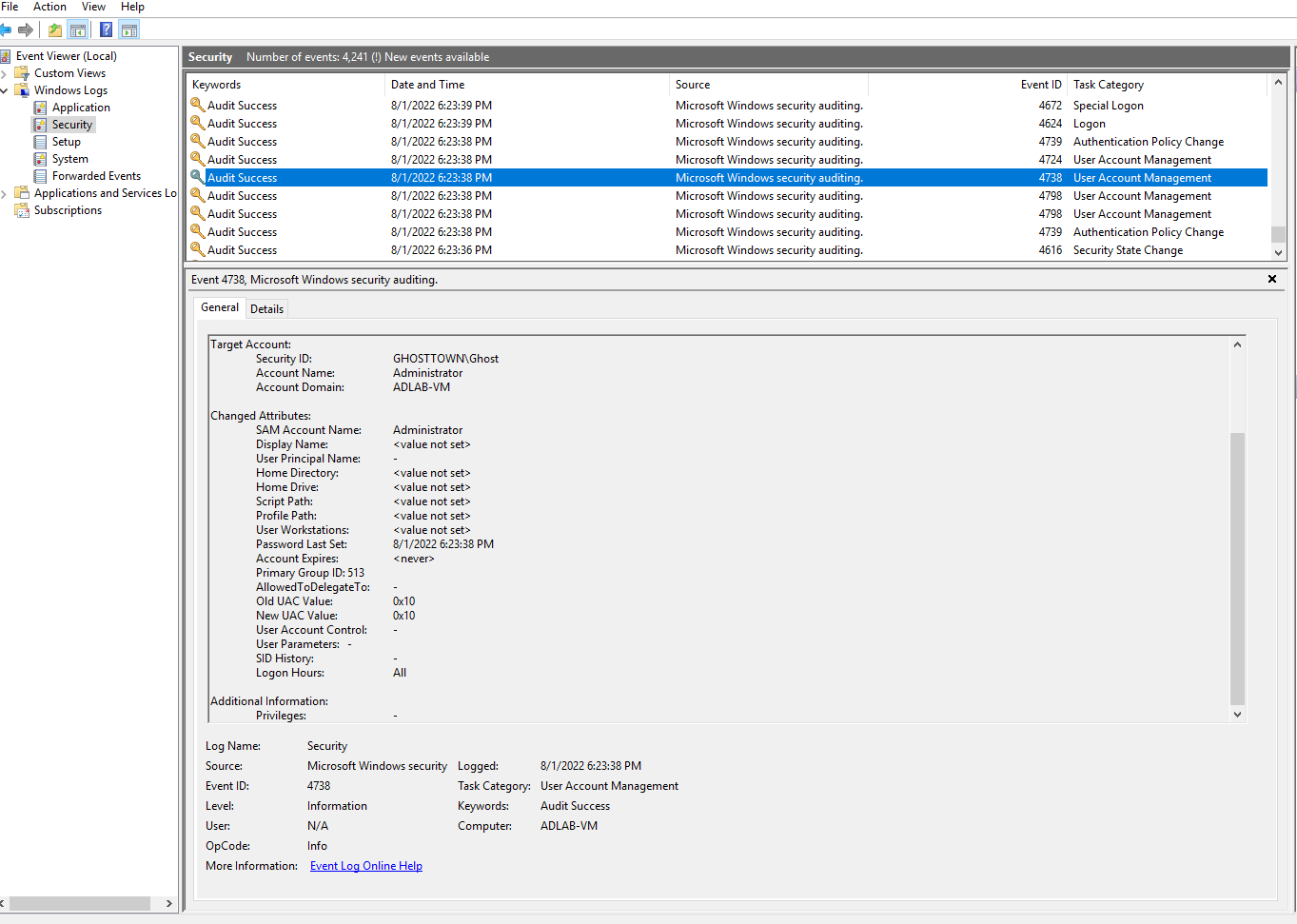
Windows Event Log analysis

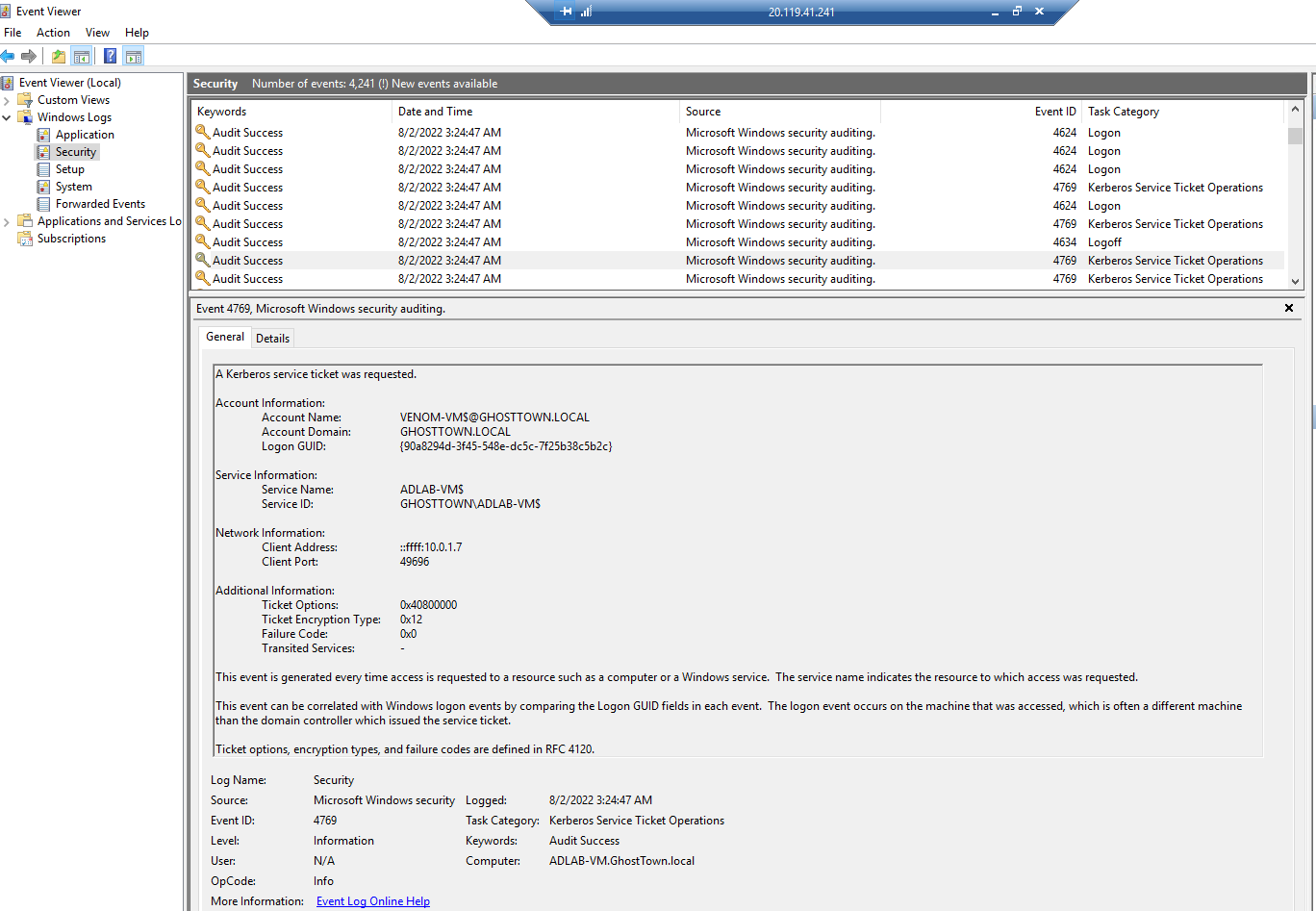
To locate the security logs. Go to search 🡪 Event Viewer 🡪 Security Logs



From looking at the current activity going on I see there has been a lot of logons and signoffs which is expected behavior as I was doing my Active Directory lab using this VM.

From the General Section I can tell the account/user name, domain where it occurred in this example on my Domain controller VM. It also provides me with a little summary of the event ID Found





Looking more closely at the logs I found other events such as user account management or Kerberos service ticket operations. If I didn’t know the activity was expected either one of these could indicate an incident or attack.

Looking at the user management log we can get a user id and a time that such activity occurred and cross reference with normal behavior baseline. If it falls outside the lines, we can use this information to start an investigation to see what user “x” was up to.

Potential Malicious Activity:

Downloading and installing Malware/ Ransomware

Exfiltrating/Deletion Organizations Data Secrets/ applications