Tues 4.15pm Monterey

Scribing Template -Tues., Nov 12, 2013 at 4:15pm - Monterey Room

TOPIC: Failed Authentication Counter

CONVENER:

SCRIBE:

# of ATTENDEES:

MAIN ISSUES DISCUSSED:

ACTIVITIES GOING FORWARD / NEXT STEPS:

SESSION NOTES

No easy way to monitor for specific events to determine when a person’s group membership should be changed from Silver to Bronze. Not easy to reduce LOA based on NTLM events.

- Use an audit to force the issue when proposing that passwords need to expire.
- The downside to using auditors, is that they are box checkers. “If you don’t have a password that expires, then you fail."

Is there a way to create a Failed Authentication Counter as a way of expiring passwords? This is a risk-based policy. There needs to be a policy for when to downgrade access. One way to determine the different types of events that might be useful to understand when creating a policy is to use Splunk or Gulp with custom reports.

There are simple attacks on teachers if there is a password lockout policy based on failed attempts. The student only needs to know the profs usernames. Usernames are readily accessible on campus.

What are the best ways to look at the traffic being generated to look for failures?

There should be a Wiki page to document the different queries that can be used to identify failed authN attempts.

It’s bad user experience to make people change their password every 90 days. For Bronze, it is a better UX to have the password expire after N attempts.

Berkley - chat with Ben for details of their implementation.