Review of Multifactor Authentication

Demo

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission.

Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM20-0577

Instructor: In this demonstration we're going to review multi-factor authentication on AWS, along with setting up a user and group within the IAM console. So first let's search for MFA. It helps us out and takes us to IAM. You see, we've already deleted our root access keys. We'll go ahead and click on this and review the note here that just informs us about the risks associated with root access keys and the power that they would have if they were to fall into the wrong hands.

But let's go ahead and enable MFA. You can see there's some options here using a YubiKey or the authenticator app, and we'll start by looking at our Authy application.

We'll set up a new identity by scanning a QR code. It adds our web services. Now we have a PIN that we're going to put in. We need two consecutive ones to verify, and we've successfully set up MFA and AWS. We'll log out and log back in to verify, and we've got our password and we got a token from our Authy app, and we've successfully used multi-factor authentication to authenticate.

Let's go back to the IAM console and complete the few things remaining here for our initial setup. We'll create a sample user. In this case, it's just a random sample user. We're going to call it our CloudTrail user. We're going to be setting up CloudTrail little bit later on. So CloudTrail user one. We're going to let them have console access, as opposed to API or programmatic access. Autogenerate the password and require them to change the password upon their first login.

We don't have a group set up, so Create a Group and we'll call it CloudTrail Users. Well, we also need some permissions for that group, so we'll find a policy related to CloudTrail and assign that to the group. So this is a default policy for CloudTrail read-only users. Let's take a quick look at that policy just to see what some of those permissions are. As we expand that out, you see it's got a few different resources that are available or that it has permissions to, and then as you drill into each one of those resources it gives you a

little bit more detail about the permissions granted to this policy.

So go out and we'll click Next. We re not going to add any tags. We got Review Our User, and we'll click Create User, and we'll close, and now we'll go back to our IAM dashboard, and you see the only thing left is to update our password policy. So let's just go ahead and check all the boxes. But for your organization, you want to try to match your corporate security guidelines and password policies into here in terms of password complexity, aging, et cetera, and now we've completed all the steps for our initial setup of our Amazon AWS account.