Unit 2 Research Project

Eddie S. Jackson

Kaplan University

IT540: Management of Information Security

Kenneth L. Flick, Ph.D.

09/30/2014
Table of Contents

Abstract .................................................................................................................................................. 3

Part I ................................................................................................................................................... 4
  Domain Controller Password Policy ................................................................................................. 4

Part II .................................................................................................................................................. 4
  Join Linux Workstation to Active Directory ..................................................................................... 4

Part III .................................................................................................................................................. 5
  Strict Password Policy ....................................................................................................................... 5

References ............................................................................................................................................. 6
Abstract

The unit two research project presents a three-part assignment that relates to security implementation. Each part of the project presents a unique challenge to demonstrate security policy. In Part I, there is a hands-on lab where the main focus of the activity is to create and apply a domain level policy. In Part II, there is second hands-on activity, which the primary emphasis is placed on joining a Linux workstation to an Active Directory domain. Finally, in Part III, there is a short essay paragraph which elaborates on the significance of having a strict password security policy. Ultimately, the research project outcome is to reinforce the fundamentals of security policy through applied knowledge and hands-on learning activities.
Unit 2 Research Project

Part I

**Domain controller password security policy.** In the first part of the assignment, a user security policy is implemented on a domain controller. See snapshots below.

Part II

**Join Linux workstation to Active Directory.** In the second part of the assignment, a Linux workstation is joined to an Active Directory domain. See snapshot below.
Part III

Strict password policy. In the third part of the assignment, the question has been raised, “Why is a strict password policy important?”

After completing the hands-on activities, it was evident that applying strict password policy is critical to the overall security of an organization. No matter how secure a network physically is, if hackers can crack end-users’ passwords, the entire network system can be compromised. Thus, measures must be taken to create the most secure passwords possible.

Several best-practices for creating a solid password policy would include: using complex passwords; do not reuse passwords; and, change passwords regularly (InformationWeek, 2012). Each of these practices should be domain-level, policy enforced for maximum effectiveness (Microsoft, n.d.). As suggested from Microsoft, the best way to enforce password security policy is by implementing a domain-based group policy. Group policy allows several password policies to be enforced throughout the selected domain. Some of the elements in group policy that can be configured for optimum password security are: enforce password history; maximum password age; minimum password age; minimum password length; and, passwords must meet complexity requirements (Microsoft, n.d.). By leveraging group policy, weak passwords such as welcome, password, and letmein, would look more like W3!c0me, P@$w0rd, and L3tm3!n.

Of course, as essential as it is to enforce password complexity, educating users is equally important. Although enforcing password complexity is a necessary part of a password policy, if an end-user writes down the password and sticks it to the monitor, security has been compromised. It is the system administrator’s or security team’s job to educate staff on the complexity requirements as well as maintaining the integrity of the password; this means that users should not write down passwords or give out passwords (Martins, 2014). In the end, strict password policies are crucial to protecting company assets.
References


