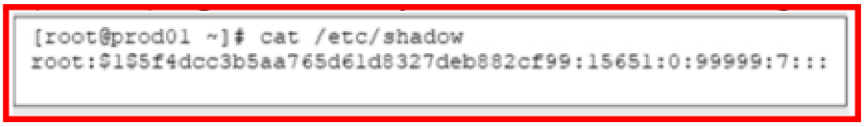
Dylan Robinson

Consultant Development Program Response

Security Warning

Upon sampling your Linux server, I came across the following entry in its **/etc/shadow** file:



Warning: This server is seriously misconfigured, and without proper remediation it will remain vulnerable due to multiple security flaws.

Context

Proper configuration of the **/etc/shadow** file is foundational to securing a Linux device. It contains hashed versions of passwords for all system accounts, as well as settings which enforce secure password management policies.

The **/etc/shadow** file consists of security information for all accounts, with one account per line. These lines separate information into fields from left to right with a **:** (colon) symbol.

Field details:

1. **Username**
2. **Encryption Type & Password**
3. **Epoch Date of Last Password Change**
4. **Minimum Password Age**
5. **Maximum Password Age**
6. **Warning Period**
7. **Inactivity Period**

Security Flaws & Remediation Procedures

1. **The root account's password is encoded using an insecure algorithm, with no salt.**

The root password has been hashed using the insecure **MD5** algorithm, as shown in the **Encryption Type & Password** field. This is shown at the beginning of the field by the **1** after the first **$** symbol. The number **1** corresponds to **MD5** encoding. Anyone with permission to view this **/etc/shadow** file may be able to decrypt the password and gain root access. This may have been caused by the PAM module **/etc/pam.d/common-password** being configured to encrypt passwords with MD5 by default. This, in and of itself, may be considered a security risk.

To remediate:

Use root privileges with **VIM** to edit a line in **/etc/pam.d/common-password**. Change the following line to replace “md5” with “yescript” (no quotes).

```
password    [success=1 default=ignore]    pam_unix.so obscure md5
```

Password reset is required for full remediation, however this will be covered in **Step 3.**

2. The password *hint* is extremely weak.

The root **password** was recovered within seconds using a basic dictionary attack with a password-recovery tool known as *hashcat*. For security purposes the root **password** will not be included in this report. Password complexity policies are an extremely important first step to achieving defense-in-depth.

To remediate:

Change the password to a combination of lower and uppercase letters, numbers, and special characters. Do not use words which exist in the dictionary. Ensure a minimum password length of 18 characters. The **obscure** string from the altered line in **Step 1** will further ensure password complexity. *Terminal commands used for further remediation are listed under **Step 3**.*

3. According to the Epoch Date field, the password has not been changed since November of 2012. In addition, the maximum password age parameter is set to its default of 99999 and the minimum password age is not set.

Enforcing password age requirements is an important strategy for an effective security posture. Regular password changes make it more difficult for malicious actors to maintain persistence in a target network. In addition, a minimum password age can help to prevent employees from circumventing your password policies by immediately changing their password back to a preferred choice. This effect can be increased by enforcing *password history requirements*, which determines how many new passwords a user must create, before circling back to a previously-used password. However, password history cannot be configured within the **/etc/shadow** file.

To remediate:

Create a new password, using the following command, then type your new secure password:

```
passwd root
```

Next, decide on password age policies, and enforce them with the command:

```
chage -m 15 -M 30 root
```

- *15 refers to the minimum password age, and 30 refers to the maximum password age.*
- *These commands must be run with root privileges.*

Conclusion

Implement these policies (at a minimum) as a security standard throughout your organization. This may be accomplished for many devices using a combination of *Active Directory Group Policy, Mobile Device Management, Microsoft Intune, and Network Access Control*.

*A final note: for Linux it is not encouraged to use the root account unless absolutely necessary. In Debian-based operating systems, **sudo** is used to temporarily issue commands with admin privileges. I can not determine the operating system used during the screenshot, so it may have been taken in an OS which does not have the sudo feature, requiring a su (switch user) to the root account. Even so, it is also recommended that a user create a non-root, administrator account for these OS's.*