Leigh Ball

CSCI 2783-Ethical Hacking

2/23/2022

**Research topic: VAX**

The VAX Operating system originated in 1977 by HP and DEC and was most widely used in the 1980s. In the early 90’s VAX was updated to comply with POSIX and renamed to OpenVAS (commonly just referred to as VAS). A feature of VAX and VAS was the use of captive accounts. Captive accounts include a group of individuals that all use the same programs, other programs that they may not need are restricted. Captive accounts by default have an auto-login with no username or password. If a password is set up for the captive account, every individual shares the same password. While this is in a sense attempting the least-privilege principle, the captive accounts end up being less secure than the user or group accounts that are available for use.

VAX/VAS documentation indicates that since these accounts typically an automatic login, they can be especially susceptible to Trojan horse or worm attacks that begin at the time a captive user logs in. The Trojan horse attack initiated by the software can give someone local or remote access to the OS and allow the bad actor to gain privileges, change files, scan for other passwords, or add additional software to the system, such as a worm. To mitigate this, the documentation emphasizes the importance of file protection and suggests that captive account users have read-only permissions. Special-Purpose Privileged captive accounts are not suggested but may be necessary if the user requires additional permissions. In addition to educating staff about security there are other measures that can be taken during account creation. This can be achieved by adding a password to the captive accounts and allowing use of the account only from the designated devices with the available qualifiers such as NOREMOTE and NONETWORK.

Despite the risk of Trojans and worms, VAS is also particularly susceptible to remote code execution, Cross-Site Scripting, and injection attacks. The most recent attack documented in CVE comes from 2016 (CVD-2016-1926), perhaps due to the relative obscurity of the OS. An XSS vulnerability included in Greenbone Security Assistant allowed bad actors to use RCE to inject HTML script. While there are only 9 incidents of VAS vulnerabilities on the CVE that date from 2011-2016, almost if not all of them include RCE and several of them use XSS or CSRF to perform injection attacks. Additionally, most of the attacks target either the OpenVAS Admin accounts or the Greenbone Security Assistant, which is the vulnerability manager software used by OpenVAS admins. As an administrator, I would not use captive accounts but rather modify group and user permissions to make sure that there are no auto-logins, this will allow incoming data to be validated. Firewalls can also be used to help mitigate malicious actors getting into your system. I also believe that educating end users about simple tactics they can use to mitigate the risk of attacks can at times be as impactful as putting permissions and protections into place.