SSH Public Key

The key

This 2048-bit RSA key can be used to grant the network vulnerability scanners that compose the selfscan.security.utexas.edu service SSH access to your servers with a user iso65 in order to facilitate credentialed scans without having to share credentials through Stache.

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApl/oEDMHKvaVObrkCA7o/gJgXAFKS6Ty+Hinu17oz/Gxd++ggtEXD3bTZ2XQbwLcCfFYQPdHo408sslZnPTbwTdBH0KWNlNvELVIKG0zTCZLtpo/o/T6AfjyCRqpaCsi+ohcbsMp8bD4e8UhLq7fG02922+p/Hk3R/lyNp8UV11VuZImdLGxOHrckmwwgUC7oKcnKdLIQ0toahj/5fStjtPbFrfdNAPi+p0rtjWe1HQo0tPEC7eFFJI/luvfrG5vzxaJYMJbdm3idIVUgo8VAFVyC9qhdkmLstmb5i2W8Ycby5qRCYdmqmbjG1ELxWpI7aYqlwtebhOicK2GSVw== iso65@rawfish.infosec.utexas.edu

Why do credentialed scans?

Network vulnerability scanners work by identifying the type and version of all network services running on scanned hosts. This data is then compared with a database of known vulnerabilities for the specific version of each service identified to generate the list of findings.

The issue with this approach is that it can be difficult to accurately identify the exact version of a service just from a connection and even more difficult to determine if specific patches have been applied. This leads to false-positives as the scanner reports vulnerabilities that may not actually exist.

Attempting to exploit possible vulnerabilities would lead to a more accurate test, but could also cause operational issues depending on the vulnerability being tested and thus is undesirable (this would be considered a penetration test rather than a vulnerability scan).

Providing credentials for a scan allows selfscan to SSH into the hosts being scanned and identify the actual services running, verify that patches have been installed for them, identify updates that have not been installed, check configuration files for common issues, see if known vulnerabilities are mitigated through configuration options, and check for common security configuration issues. This results in a more accurate and thorough scan with fewer false-positives.