5.2.7 Ensure SSH HostbasedAuthentication is disabled (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit

Run the following command and verify that output matches:

```
# grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no
```

Remediation

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/ubuntu1604/5/2/7

Last update: **2017/05/04 10:30**