NAME

ssh-keyscan — gather ssh public keys

SYNOPSIS

ssh-keyscan [**-46cHv**] [**-f** *file*] [**-p** *port*] [**-T** *timeout*] [**-t** *type*]
[*host* | *addrlist namelist*] ...

DESCRIPTION

ssh-keyscan is a utility for gathering the public ssh host keys of a number of hosts. It was designed to aid in building and verifying ssh_known_hosts files. **ssh-keyscan** provides a minimal interface suitable for use by shell and perl scripts.

ssh-keyscan uses non-blocking socket I/O to contact as many hosts as possible in parallel, so it is very efficient. The keys from a domain of 1,000 hosts can be collected in tens of seconds, even when some of those hosts are down or do not run ssh. For scanning, one does not need login access to the machines that are being scanned, nor does the scanning process involve any encryption.

The options are as follows:

-4 Forces **ssh-keyscan** to use IPv4 addresses only.

-6 Forces **ssh-keyscan** to use IPv6 addresses only.

-c Request certificates from target hosts instead of plain keys.

-f *file*
Read hosts or "addrlist namelist" pairs from *file*, one per line. If - is supplied instead of a filename, **ssh-keyscan** will read hosts or "addrlist namelist" pairs from the standard input.

-H Hash all hostnames and addresses in the output. Hashed names may be used normally by **ssh** and **sshd**, but they do not reveal identifying information should the file's contents be disclosed.

-p *port*
Port to connect to on the remote host.

-T *timeout*
Set the timeout for connection attempts. If *timeout* seconds have elapsed since a connection was initiated to a host or since the last time anything was read from that host, then the connection is closed and the host in question considered unavailable. Default is 5 seconds.

-t *type*
Specifies the type of the key to fetch from the scanned hosts. The possible values are "rsa1" for protocol version 1 and "dsa", "ecdsa", "ed25519", or "rsa" for protocol version 2. Multiple values may be specified by separating them with commas. The default is to fetch "rsa", "ecdsa", and "ed25519" keys.

-v Verbose mode. Causes **ssh-keyscan** to print debugging messages about its progress.

SECURITY

If an ssh_known_hosts file is constructed using **ssh-keyscan** without verifying the keys, users will be vulnerable to *man in the middle* attacks. On the other hand, if the security model allows such a risk, **ssh-keyscan** can help in the detection of tampered keyfiles or man in the middle attacks which have begun after the ssh_known_hosts file was created.

FILES

Input format:

```
1.2.3.4,1.2.4.4 name.my.domain,name,n.my.domain,n,1.2.3.4,1.2.4.4
```

Output format for RSA1 keys:

```
host-or-namelist bits exponent modulus
```

Output format for RSA, DSA, ECDSA, and Ed25519 keys:

```
host-or-namelist keytype base64-encoded-key
```

Where *keytype* is either “ecdsa-sha2-nistp256”, “ecdsa-sha2-nistp384”, “ecdsa-sha2-nistp521”, “ssh-ed25519”, “ssh-dss” or “ssh-rsa”.

```
/etc/ssh/ssh_known_hosts
```

EXAMPLES

Print the rsa host key for machine *hostname*:

```
$ ssh-keyscan hostname
```

Find all hosts from the file `ssh_hosts` which have new or different keys from those in the sorted file `ssh_known_hosts`:

```
$ ssh-keyscan -t rsa,dsa,ecdsa,ed25519 -f ssh_hosts | \
sort -u - ssh_known_hosts | diff ssh_known_hosts -
```

SEE ALSO

ssh(1), sshd(8)

AUTHORS

David Mazieres <dm@lcs.mit.edu> wrote the initial version, and Wayne Davison <wayned@users.sourceforge.net> added support for protocol version 2.

BUGS

It generates "Connection closed by remote host" messages on the consoles of all the machines it scans if the server is older than version 2.9. This is because it opens a connection to the ssh port, reads the public key, and drops the connection as soon as it gets the key.