

```

user@CSI:~/Tools/ssh-audit$ python ssh-audit.py homepages.econ.ed.ac.uk
# general
(gen) banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.6
(gen) software: OpenSSH 7.2p2
(gen) compatibility: OpenSSH 7.2+, Dropbear SSH 2013.62+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256@libssh.org -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp256 -- [fail] using weak elliptic curves
-- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384 -- [fail] using weak elliptic curves
-- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521 -- [fail] using weak elliptic curves
-- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) diffie-hellman-group-exchange-sha256 -- [warn] using custom size modulus (possibly weak)
-- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group14-sha1 -- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 3.9, Dropbear SSH 0.53

# host-key algorithms
(key) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
(key) rsa-sha2-512 -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256 -- [info] available since OpenSSH 7.2
(key) ecdsa-sha2-nistp256 -- [fail] using weak elliptic curves
-- [warn] using weak random number generator could reveal the key
-- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ssh-ed25519 -- [info] available since OpenSSH 6.5

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com -- [info] available since OpenSSH 6.5
-- [info] default cipher since OpenSSH 6.9.
(enc) aes128-ctr -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr -- [info] available since OpenSSH 3.7
(enc) aes256-ctr -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes128-gcm@openssh.com -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com -- [info] available since OpenSSH 6.2

# message authentication code algorithms
(mac) umac-64-etm@openssh.com -- [warn] using small 64-bit tag size
-- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com -- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 6.2
(mac) umac-64@openssh.com -- [warn] using encrypt-and-MAC mode
-- [warn] using small 64-bit tag size
-- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com -- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256 -- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-512 -- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha1 -- [warn] using encrypt-and-MAC mode
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# algorithm recommendations (for OpenSSH 7.2)
(rec) -ecdh-sha2-nistp521 -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384 -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256 -- kex algorithm to remove
(rec) -diffie-hellman-group14-sha1 -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256 -- key algorithm to remove
(rec) -hmac-sha2-512 -- mac algorithm to remove
(rec) -umac-128@openssh.com -- mac algorithm to remove
(rec) -hmac-sha2-256 -- mac algorithm to remove
(rec) -umac-64@openssh.com -- mac algorithm to remove
(rec) -hmac-sha1 -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com -- mac algorithm to remove

```