

P3.1 - SSH

1:

```
user@CS1: ~/Tools/ssh-audit
user@CS1:~/Tools/ssh-audit$ python ssh-audit.py 198.55.199.127
# general
(gsn) banner: SSH-2.0-OpenSSH_5.3
(gsn) software: OpenSSH 5.3
(gsn) compatibility: OpenSSH 5.0-6.6, Dropbear SSH 2013.56+
(gsn) compression: disabled (c198openssh.com)

# key exchange algorithms
(kex) diffie-hellman-group-exchange-sha256 -- [warn] using custom size modulus (possibly weak)
-- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group-exchange-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak hashing algorithm
(kex) diffie-hellman-group14-sha1 -- [info] available since OpenSSH 2.3.0
-- [warn] using weak hashing algorithm
(kex) diffie-hellman-group1-sha1 -- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
-- [warn] using weak 1024-bit modulus
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(kex) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28

# encryption algorithms (ciphers)
(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

# message authentication code algorithms
(mac) hmac-md5 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-sha1 -- [fail] disabled (in client) since OpenSSH 6.7, unsafe algorithm
-- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-sha1-256 -- [fail] disabled (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 4.7
-- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
-- [warn] using encrypt-and-MAC mode
(mac) hmac-sha1-512 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 2.5.0
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 2.1.0
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.47
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using encrypt-and-MAC mode
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.5.0
# algorithm recommendations (for OpenSSH 5.3)

user@CS1: ~/Tools/ssh-audit
user@CS1:~/Tools/ssh-audit$ python ssh-audit.py 206.200.248.27
# general
(gsn) banner: SSH-2.0-WeOnlyDo 2.2.0
(gsn) software: WeOnlyDo 2.2.0
(gsn) compatibility: OpenSSH 3.0+ (some functionality from 3.0.2), Dropbear SSH 2013.56+ (some functionality from 0.52)
(gsn) compression: enabled (r19b)

# key exchange algorithms
(kex) diffie-hellman-group1-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
-- [warn] using weak 1024-bit modulus
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
(kex) diffie-hellman-group14-sha1 -- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.53
-- [warn] using weak hashing algorithm
-- [info] available since OpenSSH 3.9, Dropbear SSH 0.53

# host-key algorithms
(kex) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28

# encryption algorithms (ciphers)
(enc) aes128-cbc -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak cipher mode
-- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
-- [fail] disabled (in server) since OpenSSH 3.7, Dropbear SSH 0.52
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak cipher mode
-- [warn] using weak 66-bit block size
-- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [fail] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using weak cipher mode
-- [warn] using weak 66-bit block size
-- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak cipher mode
-- [info] available since OpenSSH 2.3.0
-- [info] available since OpenSSH 3.7
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] using weak cipher mode
-- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.47
-- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
-- [fail] removed since OpenSSH 3.1
-- [warn] using weak cipher mode
-- [info] available since OpenSSH 2.3.0
-- [fail] removed since OpenSSH 3.1
-- [fail] removed since OpenSSH 3.1
-- [warn] using cipher mode
-- [info] available since OpenSSH 2.3.0
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using weak cipher mode
-- [info] available since OpenSSH 2.3.0
-- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
-- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
-- [warn] using weak cipher mode
-- [warn] using weak 66-bit block size
-- [info] available since OpenSSH 2.1.0

# message authentication code algorithms
(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
```

2:

- 198.55.199.127:
 - Software: OpenSSH
 - Versão: 5.3
- 206.200.248.27:
 - Software: WeOnlyDo
 - Versão: 2.2.9

3: De acordo com o shodan, conseguimos concluir que o WeOnlyDo apresenta 5 vulnerabilidades enquanto o OpenSSH apresenta 11. Logo, concluímos que o OpenSSH apresenta mais vulnerabilidades.

4: A vulnerabilidade mais grave é a CVE-2010-3972, com um score de 10.0 (high)).

5: Esta vulnerabilidade é baseada num overflow de um Heap-based buffer. Isto permite aos atacantes executar codigos, arbitrariamente, ou executar ataces de Deniel of Service.

Esta vulnerabilidade afeta a confidencialidade, integridade e a disponivilidade do servidor. Esta tambem permite a sua modificação não autorizada e disclosure of information.