Crackmapexec

winrm

- Command Execution
  - --no-output: do not retrieve command output
  - -x COMMAND: execute the specified command
  - -X PS_COMMAND: execute the specified PowerShell command
- options
  - --local-auth: authenticate locally to each target
  - -d DOMAIN: domain to authenticate to
  - --laps [LAPS]: LAPS authentification
  - --ignore-ssl-cert: Ignore Certificate Verification
  - --ssl: Connect to SSL Enabled WINRM
  - --port PORT: Custom WinRM port
  - --continue-on-success: continues authentication attempts even after successes
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - -H HASH [HASH ...], --hash HASH [HASH ...]: NTLM hash(es) or file(s) containing NTLM hashes
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {http,https}: use the selected server (default: https)
  - --options: display module options
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host
  - -M MODULE, --module MODULE: module to use
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options
  - -L, --list-modules: list available modules
- Credential Gathering
  - --lsa: dump LSA secrets from target systems
  - --sam: dump SAM hashes from target systems

options

- --verbose: enable verbose output
- --darrell: give Darrell a hand
- --jitter INTERVAL: sets a random delay between each connection (default: None)
- -h, --help: show this help message and exit
- -t THREADS: set how many concurrent threads to use (default: 100)
- --timeout TIMEOUT: max timeout in seconds of each thread (default: None)

smb

- Powershell Obfuscation
  - --obfs: Obfuscate PowerShell scripts
  - --amsi-bypass FILE: File with a custom AMSI bypass
  - --clear-obfscripts: Clear all cached obfuscated PowerShell scripts
- Command Execution
  - --exec-method {smbexec,mmcexec,wmiexec,atexec}: method to execute the command. Ignored if in MSSQL mode (default: wmiexec)
  - --codec CODEC: Set encoding used (codec) from the target's output (default "utf-8"). If errors are detected, run chcp.com
  - --force-ps32: force the PowerShell command to run in a 32-bit process
  - --no-output: do not retrieve command output
  - -x COMMAND: execute the specified command
  - -X PS_COMMAND: execute the specified PowerShell command
- Files
  - --put-file FILE FILE: Put a local file into remote target, ex: whoami.txt \\Windows\\Temp\\whoami.txt
  - --get-file FILE FILE: Get a remote file, ex: \\Windows\\Temp\\whoami.txt whoami.txt
- options
  - --laps [LAPS]: LAPS authentification
  - --smb-timeout SMB_TIMEOUT: SMB connection timeout, default 2 secondes
  - --continue-on-success: continues authentication attempts even after successes
  - --gen-relay-list OUTPUT_FILE: outputs all hosts that don't require SMB signing to the specified file
  - --smb-server-port SMB_SERVER_PORT: specify a server port for SMB
  - --share SHARE: specify a share (default: C$)
  - --port {139,445}: SMB port (default: 445)
  - --local-auth: authenticate locally to each target
  - -d DOMAIN: domain to authenticate to
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - -H HASH [HASH ...], --hash HASH [HAS: NTLM hash(es) or file(s) containing NTLM hashes
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {https,http}: use the selected server (default: https)
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host
  - -M MODULE, --module MODULE: module to use
  - -o MODULE_OPTION [MODULE_OPTI: module options
  - -L, --list-modules: list available modules
  - --options: display module options
- Credential Gathering
  - --user USERNTDS: Dump selected user from DC
  - --enabled: Only dump enabled targets from DC
  - --sam: dump SAM hashes from target systems
  - --lsa: dump LSA secrets from target systems
  - --ntds [{drsuapi,vss}]: dump the NTDS.dit from target DCs using the specifed method (default: drsuapi)
- Mapping/Enumeration
  - --wmi-namespace NAMESPACE: WMI Namespace (default: root\cimv2)
  - --wmi QUERY: issues the specified WMI query
  - --rid-brute [MAX_RID]: enumerate users by bruteforcing RID's (default: 4000)
  - --pass-pol: dump password policy
  - --local-groups [GROUP]: enumerate local groups, if a group is specified then its members are enumerated
  - --computers [COMPUTER]: enumerate computer users
  - --shares: enumerate shares and access
  - --sessions: enumerate active sessions
  - --disks: enumerate disks
  - --loggedon-users-filter LOGGEDON_USERS_FILTER: only search for specific user, works with regex
  - --loggedon-users: enumerate logged on users
  - --users [USER]: enumerate domain users, if a user is specified than only its information is queried.
  - --groups [GROUP]: enumerate domain groups, if a group is specified than its members are enumerated
- Spidering
  - --only-files: only spider files
  - --depth DEPTH: max spider recursion depth (default: infinity & beyond)
  - --regex REGEX [REGEX ...]: regex(s) to search for in folders, filenames and file content
  - --pattern PATTERN [PATTERN ...]: pattern(s) to search for in folders, filenames and file content
  - --spider SHARE: share to spider
  - --spider-folder FOLDER: folder to spider (default: root share directory)
  - --content: enable file content searching
  - --exclude-dirs DIR_LIST: directories to exclude from spidering

ldap

- Retrieve useful information on the domain
  - --trusted-for-delegation: Get the list of users and computers with flag TRUSTED_FOR_DELEGATION
  - --password-not-required: Get the list of users with flag PASSWD_NOTREQD
  - --admin-count: Get objets that had the value adminCount=1
  - --users: Enumerate enabled domain users
  - --groups: Enumerate domain groups
  - --gmsa: Enumerate GMSA passwords
  - --get-sid: Get domain sid
- options
  - --local-auth: authenticate locally to each target
  - -d DOMAIN: domain to authenticate to
  - --no-smb: No smb connection
  - --port {636,389}: LDAP port (default: 389)
  - --continue-on-success: continues authentication attempts even after successes
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - -H HASH [HASH ...], --hash HASH [HASH ...]: NTLM hash(es) or file(s) containing NTLM hashes
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {http,https}: use the selected server (default: https)
  - --options: display module options
  - -L, --list-modules: list available modules
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host
  - -M MODULE, --module MODULE: module to use
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options
- Retrevie hash on the remote DC
  - --kerberoasting KERBEROASTING: Get TGS ticket ready to crack with hashcat
  - --asreproast ASREPROAST: Get AS_REP response ready to crack with hashcat

mssql

- Files
  - --put-file FILE FILE: Put a local file into remote target, ex: whoami.txt C:\Windows\Temp\whoami.txt
  - --get-file FILE FILE: Get a remote file, ex: C:\Windows\Temp\whoami.txt whoami.txt
- Powershell Obfuscation
  - --obfs: Obfuscate PowerShell scripts
  - --clear-obfscripts: Clear all cached obfuscated PowerShell scripts
- options
  - --continue-on-success: continues authentication attempts even after successes
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - -q QUERY, --query QUERY: execute the specified query against the MSSQL DB
  - --port PORT: MSSQL port (default: 1433)
  - -H HASH [HASH ...], --hash HASH [HASH ...]: NTLM hash(es) or file(s) containing NTLM hashes
  - --local-auth: authenticate locally to each target
  - -d DOMAIN: domain name
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {http,https}: use the selected server (default: https)
  - --options: display module options
  - -L, --list-modules: list available modules
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host
  - -M MODULE, --module MODULE: module to use
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options
- Command Execution
  - -X PS_COMMAND: execute the specified PowerShell command
  - -x COMMAND: execute the specified command
  - --force-ps32: force the PowerShell command to run in a 32-bit process
  - --no-output: do not retrieve command output

ssh

- Command Execution
  - --no-output: do not retrieve command output
  - -x COMMAND: execute the specified command
- options
  - --continue-on-success: continues authentication attempts even after successes
  - --port PORT: SSH port (default: 22)
  - --key-file KEY_FILE: Authenticate using the specified private key. Treats the password parameter as the key's passphrase.
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {https,http}: use the selected server (default: https)
  - --options: display module options
  - -L, --list-modules: list available modules
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options
  - -M MODULE, --module MODULE: module to use
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host

rdp

- Screenshot
  - --screenshot: Screenshot RDP if connection success
  - --screentime SCREENTIME: Time to wait for desktop image
  - --res RES: Resolution in "WIDTHxHEIGHT" format. Default: "1024x768"
- options
  - --local-auth: authenticate locally to each target
  - -d DOMAIN: domain to authenticate to
  - --nla-screenshot: Screenshot RDP login prompt if NLA is disabled
  - --rdp-timeout RDP_TIMEOUT: RDP timeout on socket connection
  - --port PORT: Custom RDP port
  - --continue-on-success: continues authentication attempts even after successes
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - -H HASH [HASH ...], --hash HASH [HASH ...]: NTLM hash(es) or file(s) containing NTLM hashes
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {http,https}: use the selected server (default: https)
  - --options: display module options
  - -L, --list-modules: list available modules
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host
  - -M MODULE, --module MODULE: module to use
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options

ftp

- options
  - -continue-on-success: continues authentication attempts even after successes
  - --port PORT: FTP port (default: 21)
  - --no-bruteforce: No spray when using file for username and password (user1 => password1, user2 => password2
  - --connectback-host CHOST: IP for the remote system to connect back to (default: same as server-host)
  - --server-port PORT: start the server on the specified port
  - --server-host HOST: IP to bind the server to (default: 0.0.0.0)
  - --server {https,http}: use the selected server (default: https)
  - --options: display module options
  - -L, --list-modules: list available modules
  - -o MODULE_OPTION [MODULE_OPTION ...]: module options
  - -M MODULE, --module MODULE: module to use
  - -h, --help: show this help message and exit
  - -id CRED_ID [CRED_ID ...]: database credential ID(s) to use for authentication
  - -u USERNAME [USERNAME ...]: username(s) or file(s) containing usernames
  - -p PASSWORD [PASSWORD ...]: password(s) or file(s) containing passwords
  - -k, --kerberos: Use Kerberos authentication
  - --use-kcache: Use Kerberos authentication from ccache file (KRB5CCNAME)
  - --export EXPORT [EXPORT ...]: Export result into a file, probably buggy
  - --aesKey AESKEY [AESKEY ...]: AES key to use for Kerberos Authentication (128 or 256 bits)
  - --kdcHost KDCHOST: FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
  - --gfail-limit LIMIT: max number of global failed login attempts
  - --ufail-limit LIMIT: max number of failed login attempts per username
  - --fail-limit LIMIT: max number of failed login attempts per host

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles
www.hackingarticles.in