

Forum:[Hack Forums](#)

Thread: [RDP Reaper | RDP Hacker KIT](#)

anonav - February 5, 2025, 11:08 pm

This tool is designed for brute-forcing Remote Desktop Protocol (RDP) credentials across multiple IPs or IP ranges. It includes features for credential validation, target scanning, making it a full-fledged suite for hacking RDPs

Breakdown of Features:

Bruteforce to IP List

Loads individual IP addresses for brute-force attempts.

Allows login, password, and login:password combination inputs.

Settings include thread count, timeout, and RDP port (default 3389).

Statistics track success, failures, and progress.

Bruteforce to IP Ranges

Similar to the first but operates on IP ranges instead of single addresses.

Can systematically attempt logins across multiple subnets.

Checker

Verifies whether a set of credentials work on a given machine.

Options for:

“Change NLA” (likely to bypass Network Level Authentication).

“Use screenshot” (potentially captures a visual confirmation of login success).

“Use Geo IP” (tracks geolocation of IPs).

“Use Ping” (tests if a host is online before attacking).

“Use blacklists” (likely avoids attacking known honeypots or flagged IPs).

This is a RDP brute-force tool that supports mass scanning, checking, and account validation. It includes optimizations for efficiency (high thread count, timeout settings) and stealth (blacklist avoidance, ping checks)

DOWNLOADBreakdown of Features:

Bruteforce to IP List

Loads individual IP addresses for brute-force attempts.

Allows login, password, and login:password combination inputs.

Settings include thread count, timeout, and RDP port (default 3389).

Statistics track success, failures, and progress.

Bruteforce to IP Ranges

Similar to the first but operates on IP ranges instead of single addresses.

Can systematically attempt logins across multiple subnets.

Checker

Verifies whether a set of credentials work on a given machine.

Options for:

“Change NLA” (likely to bypass Network Level Authentication).

“Use screenshot” (potentially captures a visual confirmation of login success).

“Use Geo IP” (tracks geolocation of IPs).

“Use Ping” (tests if a host is online before attacking).

“Use blacklists” (likely avoids attacking known honeypots or flagged IPs).

This is a RDP brute-force tool that supports mass scanning, checking, and account validation. It includes optimizations for efficiency (high thread count, timeout settings) and stealth (blacklist

avoidance, ping checks)

[deleted]

Bastille - February 6, 2025, 12:59 am

From the [Help Docs](#) :

16. Off-Site Communication contact methods not allowed to be posted by non-upgraded members. This includes the posting of your email, Discord, or Telegram account names.

13. No advertising or posting of Discord or Telegram channels unless you are in Vendor group.

Don't try to circumvent the rules

bobbyzzz - July 27, 2025, 1:49 am

So I've been messing around with RDP bruteforce lately — nothing fancy, just testing stuff in lab environments for a personal red team lab setup.

Most of the tools I found were either too outdated, slow, full of bugs, or just didn't work with custom credential lists and threading the way I needed. I tried Hydra, Crowbar, Ncrack, and even a few GitHub scripts... but either they were clunky or just straight up broken for RDP.

After a few days of testing, I finally came across this little gem:

rensii - fast rdp

It's clean, Python-based, super lightweight, and has exactly what I needed:

- Multithreading (fast as hell)
- Works with my credential dumps
- Timeout and connection handling that actually works
- Simple CLI, no bloat

It's not one of those bloated "all-in-one" tools — it just does RDP and does it well.

Figured I'd drop it here in case someone else is on the same hunt I was. Hope it helps.

x64x86 - August 6, 2025, 9:57 am

(Jul 27, 2025 01:49 AM)bobbyzzz Wrote: [\[CITE\]](#) So I've been messing around with RDP bruteforce lately — nothing fancy, just testing stuff in lab environments for a personal red team lab setup.

Most of the tools I found were either too outdated, slow, full of bugs, or just didn't work with custom credential lists and threading the way I needed. I tried Hydra, Crowbar, Ncrack, and even a few GitHub scripts... but either they were clunky or just straight up broken for RDP.

After a few days of testing, I finally came across this little gem:

rensii - fast rdp

It's clean, Python-based, super lightweight, and has exactly what I needed:

- Multithreading (fast as hell)
- Works with my credential dumps
- Timeout and connection handling that actually works
- Simple CLI, no bloat

It's not one of those bloated "all-in-one" tools — it just does RDP and does it well.

Figured I'd drop it here in case someone else is on the same hunt I was. Hope it helps.

Don't deceive users. rensii - fast rdp is a very old brute from StasM, which is already 15 years old. Your schoolboy-rensii just found this brute somewhere and re-uploaded it to GitHub ?