

Forum:[Hack Forums](#)

Thread: [Spirit | Network Pentest Tools | SSH | BRUTE | BANNER | EXPLOIT | All-in-One](#)

aog7 - May 25, 2024, 10:24 am

Spirit - Network Pentest Tools

I wrote an SSH brute forcer for passwords and keys which also includes a banner grabber and other pentesting tools.

Please try it and let me know what do you think, thank you!

PS: I'm not allowed to post links yet, though you can easily find it on github: /theaog/spirit

Code NAME:

Spirit - Penetration Testing Tools

USAGE:

./spirit --help

COMMANDS:

main:

brute, B performs brute-force password guessing against ssh servers
brutekey, K performs brute-force using a private key (default id_rsa) on users from your

p.lst file.

banner, b grab SSH version (banner) without performing a login
proxybanner, pb, bb, b2 BETA: improved SSH version grabber - faster, more accurate, Terminal UI and socks5 support. Provide SOCKS5:IP:PORT in proxy.lst file.

autossh, o, as auto-ssh on all found.lst hosts and run commands or upload files
scan, s open ports network scanner, designed for LAN scans (no root required)
masscan, ms masscan automation using zone.lst file: ./spirit ms --help
autobrute, ab masscan->banner->brute on random ports in a forever loop
parse, p parses masscan/nmap -oG output from open.lst and generates h.lst in

IP:PORT format

ports, P generate random ports in 1-65535 range avoiding duplicates
zap, z clean connection logs from wtmp/utmp/lastlog/auth.log/audit.log
passwd, pw parses /etc/passwd file and generates random passwords for uncommon

users

abuse check your host IP against abuse report databases
exploit, e tries multiple CVE on local host until one works (includes Gitlab exploit

subcmd)

encrypt, E activates encryption for your passfile (p.lst)
bot IRC bot that monitors system changes and issues NOTICE on channel

support:

upgrade, u, update download the latest version with new features and bug fixes
register, r register your Spirit license on this server
partner, pp become a Spirit Partner, get 10% off earn up to 30% XMR
reset, R remove ALL your registered servers and start fresh
buy buy a license to donate & support this project (XMR only) -- thank you!

GLOBAL OPTIONS:

--terms display terms & conditions (default: false)
--motd (default: true)
--help, -h show help

COPYRIGHT:

(c) The Armor of God

DramaKing - *May 25, 2024, 11:13 am*

Please delete this spam post.

aog7 - *May 25, 2024, 11:19 am*

(May 25, 2024 11:13 AM)DramaKing Wrote: [\[CITE\]](#) Please delete this spam post.
I cannot find any delete button :/