

Forum:[Hack Forums](#)

Thread: [removed](#)

Mad76e - May 21, 2014, 3:03 pm

removed due to unknown reasons

Sorry guys

Mad76e - June 3, 2014, 9:41 am

An big update to the thread.. Now its not as noobish as before

matthew28394 - June 5, 2014, 11:10 am

Thank you OP this is a really helpful guide

Also people like using phone numbers if you area code is (321) use that then generate all combos of the other 7 numbers.

TheGrayAviator - May 28, 2015, 4:42 am

If you really want to create your own customized wordlist, you could use CeWL.

This tool will crawl through a given URL and create a file based on the contents of the website.

<https://digi.ninja/projects/cewl.php>

Mad76e - May 28, 2015, 4:49 am

Thanks TheGrayAviator.. That's really helpful

TheGrayAviator - May 28, 2015, 5:01 am

(May 28, 2015 04:49 AM)mad76e™ Wrote: [\[CITE\]](#) Thanks TheGrayAviator.. That's really helpful
No worries, its a great little tool and it does a great job. I've used it a couple of times before. In addition, if your target has a website, it could prove really useful.

agentshield - May 28, 2015, 8:45 am

may i add, if your target is an AP. and the ssid is factory default. chances are the owner of the AP never accessed the router page and has not changed anything which means the network key is also the default 16 alphanumerical.

Good luck with cracking that.

imagine the following. i ran wordlist1.txt on handshake. no passphrase found. so i run wordlist 2 and 3 and 4, no passphrase found. so then i download wordlist 5. .

is there a way to compare word list5 with wordlist 1 2 3 and 4 to remove repeating words on wordlist 5?

agentshield - May 28, 2015, 9:13 am

(May 28, 2015 09:00 AM)mad76e™ Wrote: [\[CITE\]](#) It doesn't work like that.

1. First you Google the vendor to find out if the router has a known vuln, (exposed key through MAC and ESSID)
2. Then we look if the router has WPS enabled, if so, does the router has an vuln chipset, then we

use Dust WPApXie Attack

3. Run Reaver

4. If all fails, then we run a wordlist against it. (all mine are about 100gb and take 3 days to run

5. if that fails, we take the next router. The world is full of routers...

Wordlists are a last resort if everything else fails so you telling me that there is no way to compare 2 text files for duplicate words?

Mad76e - May 28, 2015, 9:34 am

Damn... I misread.. Yeah you do like this

To merge all files to one

```
cat *.lst >> bigfile.lst
```

```
sort -u passwordfile.lst > clean_passwordfile.lst
```

^ = Unique wordlist

There is one other to check through multiple filelists for duplicates, but right now it has slipped my mind

agentshield - May 28, 2015, 11:45 am

(May 28, 2015 09:34 AM)mad76e™ Wrote: [\[CITE\]](#) Damn... I misread.. Yeah you do like this

To merge all files to one

```
cat *.lst >> bigfile.lst
```

```
sort -u passwordfile.lst > clean_passwordfile.lst
```

^ = Unique wordlist

There is one other to check through multiple filelists for duplicates, but right now it has slipped my mind thanks for that. it will prove usefull.

TheGrayAviator - May 28, 2015, 7:01 pm

(May 28, 2015 09:34 AM)mad76e™ Wrote: [\[CITE\]](#) Damn... I misread.. Yeah you do like this

To merge all files to one

```
cat *.lst >> bigfile.lst
```

```
sort -u passwordfile.lst > clean_passwordfile.lst
```

^ = Unique wordlist

There is one other to check through multiple filelists for duplicates, but right now it has slipped my mind

Or you could use WLM (word list manipulator) to optimize it for you.

Tr0janVirus - June 18, 2015, 11:55 pm

Can you please PM me the link to download crunch for mac ?

jfcnumberone - April 4, 2016, 1:50 am

(Jun 18, 2015 11:55 PM)Tr0janVirus Wrote: [\[CITE\]](#) Can you please PM me the link to download crunch for mac ?

<http://macappstore.org/crunch/>

you need to install brew first if you dont have it