Outras Ferramentas para DNS Recon

+ Temos o dig que funciona de maneira semelhante à do host

```
dig -t ns businesscorp.com.br +short
```

```
dig -t mx businesscorp.com.br +short
```

```
dig www.businesscorp.com.br +short
```

```
dig rh.businesscorp.com.br +short
```

```
dig -t axfr businesscorp.com.br @ns2.businesscorp.com.br
```

→ para realizar a transferência de zona, devemos acrescentar esse @

+ Outra ferramenta bem conhecida é o dnsenum

```
dnsenum --enum businesscorp.com.br
```

+ Há também o dnsrecon

```
dnsrecon -d businesscorp.com.br
```

+ fierce

```
fierce -dns businesscorp.com.br
```

+ Cada ferramenta dessas vem com uma wordlist

```
cd /usr/share/dnsenum
```