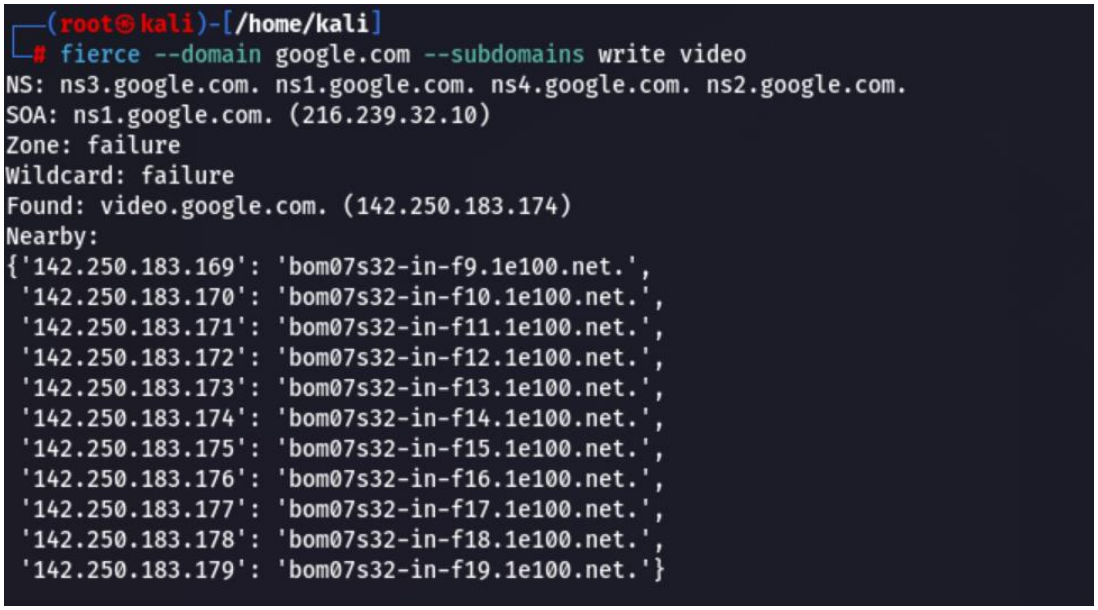
Fierce

Fierce is a semi-lightweight scanner that helps locate non-contiguous IP space and hostnames against specified domains. It's really meant as a pre-cursor to nmap, unicornscan, nessus, nikto, etc, since all of those require that you already know what IP space you are looking for. This does not perform exploitation and does not scan the whole internet indiscriminately. It is meant specifically to locate likely targets both inside and outside a corporate network.

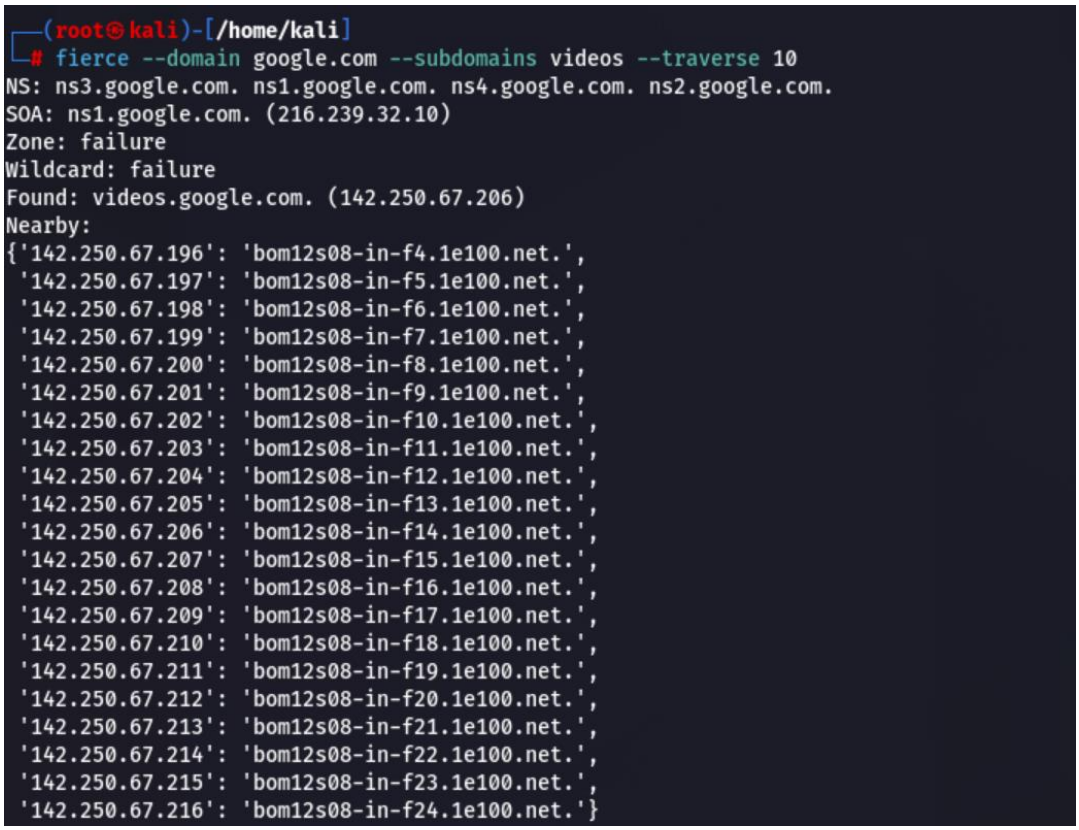
Because it uses DNS primarily you will often find mis-configured networks that leak internal address space. That's especially useful in targeted malware.

Example: -

1. We are performing a simple scan using the subdomain words which include write, videos.



2. Here we Traverse IPs near discovered domains to search for contiguous blocks with the –traverse flag.



3. Here we attempt an HTTP connection on domains discovered with the –connect flag.

```
┌──(root㉿kali)-[/home/kali]
└─# fierce --domain google.com --subdomains mail --connect
NS: ns3.google.com. ns1.google.com. ns4.google.com. ns2.google.com.
SOA: ns1.google.com. (216.239.32.10)
Zone: failure
Wildcard: failure
Found: mail.google.com. (142.250.183.37)
HTTP connected:
[('Location', 'http://www.google.com/'),
 ('Content-Type', 'text/html; charset=UTF-8'),
 ('Content-Security-Policy-Report-Only',
  "object-src 'none';base-uri 'self';script-src 'nonce-KZwBL0NJd6yNAXspsYV-RA' "
  "'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: "
  'http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp'),
 ('Date', 'Mon, 27 May 2024 08:48:21 GMT'),
 ('Expires', 'Wed, 26 Jun 2024 08:48:21 GMT'),
 ('Cache-Control', 'public, max-age=2592000'),
 ('Server', 'gws'),
 ('Content-Length', '219'),
 ('X-XSS-Protection', '0'),
 ('X-Frame-Options', 'SAMEORIGIN')]
Nearby:
{'142.250.183.32': 'bom12s11-in-f0.1e100.net.',
 '142.250.183.33': 'bom12s11-in-f1.1e100.net.',
 '142.250.183.34': 'bom12s11-in-f2.1e100.net.',
 '142.250.183.35': 'bom12s11-in-f3.1e100.net.',
 '142.250.183.36': 'bom12s11-in-f4.1e100.net.',
 '142.250.183.37': 'bom12s11-in-f5.1e100.net.',
 '142.250.183.38': 'bom12s11-in-f6.1e100.net.',
 '142.250.183.39': 'bom12s11-in-f7.1e100.net.',
 '142.250.183.40': 'bom12s11-in-f8.1e100.net.',
 '142.250.183.41': 'bom12s11-in-f9.1e100.net.',
 '142.250.183.42': 'bom12s11-in-f10.1e100.net.'}
```

4. We have exchange speed for breadth with the –wide flag, which looks for nearby domains on all IPs of the /24 of a discovered domain.

```
└─# fierce --domain google.com --wide
NS: ns3.google.com. ns1.google.com. ns4.google.com. ns2.google.com.
SOA: ns1.google.com. (216.239.32.10)
Zone: failure
Wildcard: failure
Found: 1.google.com. (142.250.192.110)
Nearby:
{'142.250.192.0': 'bom12s14-in-f0.1e100.net.',
 '142.250.192.1': 'bom12s14-in-f1.1e100.net.',
 '142.250.192.10': 'bom12s14-in-f10.1e100.net.',
 '142.250.192.100': 'bom12s17-in-f4.1e100.net.',
 '142.250.192.101': 'bom12s17-in-f5.1e100.net.',
 '142.250.192.102': 'bom12s17-in-f6.1e100.net.',
 '142.250.192.103': 'bom12s17-in-f7.1e100.net.',
 '142.250.192.104': 'bom12s17-in-f8.1e100.net.',
 '142.250.192.105': 'bom12s17-in-f9.1e100.net.',
 '142.250.192.106': 'bom12s17-in-f10.1e100.net.',
 '142.250.192.107': 'bom12s17-in-f11.1e100.net.',
 '142.250.192.108': 'bom12s17-in-f12.1e100.net.',
 '142.250.192.109': 'bom12s17-in-f13.1e100.net.',
 '142.250.192.11': 'bom12s14-in-f11.1e100.net.',
 '142.250.192.110': 'bom12s17-in-f14.1e100.net.',
 '142.250.192.111': 'bom12s17-in-f15.1e100.net.',
 '142.250.192.112': 'bom12s17-in-f16.1e100.net.',
 '142.250.192.113': 'bom12s17-in-f17.1e100.net.',
 '142.250.192.114': 'bom12s17-in-f18.1e100.net.',
 '142.250.192.115': 'bom12s17-in-f19.1e100.net.',
 '142.250.192.116': 'bom12s17-in-f20.1e100.net.',
 '142.250.192.117': 'bom12s17-in-f21.1e100.net.',
 '142.250.192.118': 'bom12s17-in-f22.1e100.net.',
 '142.250.192.119': 'bom12s17-in-f23.1e100.net.',
 '142.250.192.12': 'bom12s14-in-f12.1e100.net.',
 '142.250.192.120': 'bom12s17-in-f24.1e100.net.',
 '142.250.192.121': 'bom12s17-in-f25.1e100.net.',
 '142.250.192.122': 'bom12s17-in-f26.1e100.net.',
 '142.250.192.123': 'bom12s17-in-f27.1e100.net.',
```