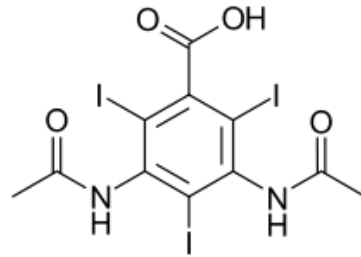


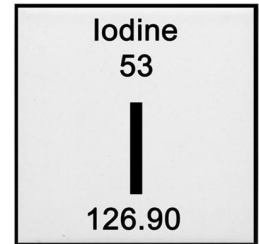
Iodine

Tricky Encapsulation for Stealthy Tunnels



What is Iodine?

- Tunnels IP over DNS
 - *DNS protocol is used to resolve domain names into IP addresses*
- Cross-platform implementation
 - *Use it on Linux, macOS, Windows, Android*
- Can bypass network blocks in many cases
 - *Firewalls, proxies, other types of network filters*



Concept: The OSI Model

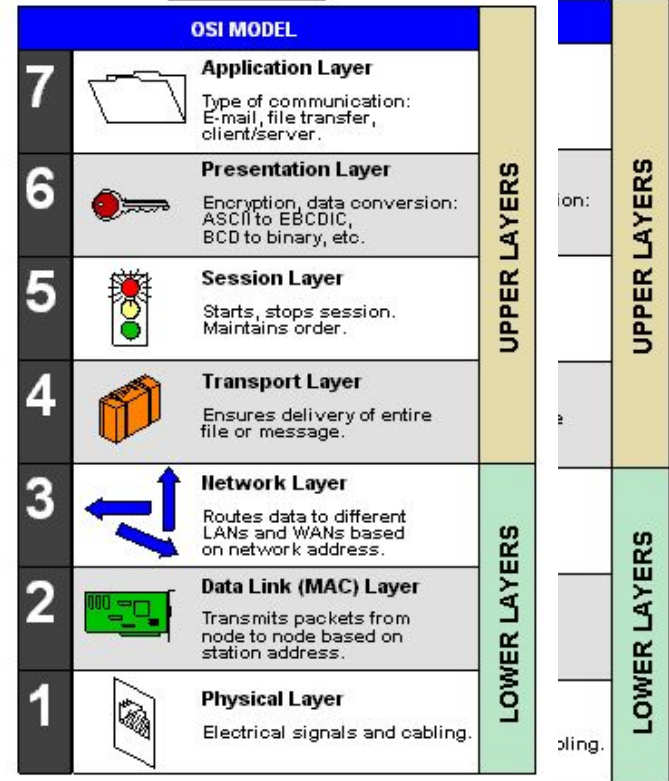


Iodine takes IPv4 traffic (layer 3) and encapsulates it in DNS queries (layer 7)

Through this link, you can tunnel upper-layer applications that use IP (think: everything!)

DNS, SSH, HTTP etc

TCP/IP



Demo Time!

Iodine - Useful Links

Code:

- <https://github.com/yarrick/iodine>
- <https://code.kryo.se/iodine/>

Guides:

- <https://gist.github.com/nukeador/7483958>
- <https://calebmadrigal.com/dns-tunneling-with-iodine/>
- [https://en.wikipedia.org/wiki/Encapsulation_\(networking\)](https://en.wikipedia.org/wiki/Encapsulation_(networking))

DEFCON Talks:

- <https://www.youtube.com/watch?v=IkXG14MA3M4>

Similar Projects

- **Dns2tcp**
 - Possibly better performance and/or easier setup, less client-side tuning needed
 - <https://www.aldeid.com/wiki/Dns2tcp>
- **Heyoka**
 - <http://heyoka.sourceforge.net/>
- **Netcross**
 - <https://sourceforge.net/p/netcross/wiki/Home/>