

Tor + Freenode

Free at last, free at last

Concepts

- ▶ Tor - anonymity online
- ▶ JanusVM - vpn server tunneling everything over tor
- ▶ Freenode - irc.freenode.net
- ▶ TwistedMatrix - awesome lib for writing custom clients/servers in python
- ▶ SASL - Simple Authentication and Security Layer
- ▶ IRC - method of moving ascii porn from one linux user to another

Why

- ▶ Freenode is one of the most, if not the most prevalent IRC provider on the planet - but never allowed tor'd users...until now
- ▶ Evil - trolling, general harassment, IRC bots
- ▶ Good - anonymous assistance and collaboration, IRC bots

IRC Bots

- ▶ Providing help or cataloging data
- ▶ Performing routine/mundane tasks
- ▶ Sifting through IRC garbage for that one golden turd

Anonymity Online

- ▶ We live in a gray area, and sometimes you gotta go dark
- ▶ Censorship issues
- ▶ SOPA, PIPA, ACTA, RIAA, MPAA, Sony, EMG, WebSherriff, and a whole host of other A\$\$HOLES

Connection Information

- ▶ p4fsi4ockecnea7l.onion is the URL; traditional URL doesn't work
- ▶ Linux setup - Debian or CentOS:
 - ▶ Apt-get install pptp-networkmanager-gnome
 - ▶ Setup VPN with JanusVM creds
- ▶ JanusVM:
 - ▶ Download from http://www.janusvm.com/JanusVM_01_2010.zip
 - ▶ Use vmware player or ESXi+converter to upload to server

Code Libraries Used

- ▶ TwistedMatrix - great for rolling your own protocols wrapped in SSL
- ▶ Zope - get this if easy_install twisted doesn't install zope as well
- ▶ BeautifulSoup - wget on 'roids

SASL Handshake

- ▶ You: CAP REQ :sasl\r\nNICK nick\r\nUSER nick irc.freenode.net 1 :Abvious Foggot\r\n
- ▶ Them: CAP * ACK :sasl
- ▶ You: AUTHENTICATE PLAIN\r\n (or AUTHENTICATE DIGEST-MD5)
- ▶ Them: AUTHENTICATE+
- ▶ You: “AUTHENTICATE
”+self.transport.write(base64.encodestring(“nick\x00nick\x00password”))
- ▶ Them: 903 nick :SASL authentication successful
- ▶ You: CAP END\r\n

- ▶ IMPORTANT: REMEMBER \r\n - server will timeout if it doesn't see the newline chars

DEMO TIME!!!