Autonomously Bypassing VoIP Filters With Asterisk: Let Freedom Ring

The Last HOPE
July 18th 2008, 5pm

Blake Cornell, Jeremy McNamara

For the next 55 minutes we will be discussing

- General VoIP censorship
- Government censorship in china
- Google's role in censorship
- Why am I here
- Technical overview of VoIP Filters
- Firewalls
  - SIP
  - IAX
  - DUNDI
- ACL's
- IAX Ping Poker

General VoIP Censorship

There has been a trend for foreign governments to censor their populous from information exchanges. Some effects are quite obvious, the primary example being a dead internet telephone. There have been reports of VoIP outages in more then 15 countries!

Government Censorship in China

VoIP has been restricted in China from 2006 till 2008. The Chinese government has promised VoIP providers that they will have to become 'certified' to conduct business. As well, if a citizen of China were to not use one of these providers, their VoIP phone may be 'disconnected' from the outside world, or worse.

Not only would this limit native citizens, it would also hinder international business executives as well.

Government Censorship in China

Due to these and other circumstances, some groups have even been spamming proxy like tools to lists of users within china. Their hopes are to allow someone the ability to use the attached software to release themselves from the grips of Government sponsored censorship.

Breaking Down the 'Great Firewall of China

By Jonathan Serrie

Friday, June 20, 2008

“As Beijing readies itself for the Olympic Games in August, Chinese dissidents living in the U.S. have launched an attack on the country's so-called "Great Firewall," which prohibits its citizens from having full access to the Internet.”

Google's Role in Censorship

There have been a series of Corporations registered within US territories that seem to helplessly cooperate with censoring foreign governments. Clear cut example, Google.

China's Google Search Engine to Be Censored

Associated Press

Wednesday, January 25, 2006

“Online search engine leader Google Inc. has agreed to censor its results in China, adhering to the country's free-speech restrictions in return for better access in the Internet's fastest growing market.”

Google's Role in Censorship

Which is why Google was harshly criticized during congressional hearings.

Google Blasted for Bowing to Chinese Government

Associated Press

Friday, January 27, 2006

“Google's decision to filter sensitive topics from Web searches in China is a major triumph for the regime's campaign to have the Internet censor itself, observers said Thursday, amid mounting criticism of the move.”

Google's Role in Censorship

Would you believe that Google took an ethical stance on it? At least when they get negative press.

Google Continues to Fight Global Internet Censorship

Tuesday, June 26, 2007
Associated Press

“Once relatively indifferent to government affairs, Google Inc. is seeking help inside the Beltway to fight the rise of Web censorship worldwide.”

Why Am I Here

What could be done about censorship?

In my eyes, there are currently two routes. Legislative and the reasons why I'm here.

I'm not pleased with this type of coercion from such a successful and emulated company within American culture. Neither is Congressman Chris Smith (R-NJ).

Why Am I Here

"Global Online Freedom Act"

H.R. 275
Title: To promote freedom of expression on the Internet, to protect United States businesses from coercion to participate in repression by authoritarian foreign governments, and for other purposes.
Sponsor: Rep Smith, Christopher H. [NJ-4] (introduced 1/5/2007) Cosponsors (8)
Latest Major Action: 2/22/2008 Placed on the Union Calendar, Calendar No. 320.
House Reports: 110-481 Part 1

http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00275:

Why Am I Here

"It shall be the policy of the United States--
(1) to promote as a fundamental component of United States foreign policy ***the right of every individual to freedom of opinion and expression****, including the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers;*

(2) to use all appropriate instruments of United States influence, including diplomacy, trade policy, and export controls, to support, promote, and strengthen principles, practices, and values that ***promote the free flow of information****, including* ***through the Internet*** *and other electronic media; and*

(3) to ***deter any United States business from cooperating*** *with officials of Internet-restricting countries in effecting the political censorship of online content."*

Why Am I Here

I believe that ideals and ideas are the more significant parts of human behavior. An idea of mine concerns those who can't enact the “simple” measures required to “guarantee” connectivity through a wake of government enforced censorship.

Remember, those who have the best tools wins.

I am releasing a small Perl script that, on a basic level, allows a user the ability to determine if VoIP filtering, specifically the Asterisk's IAX protocol, is in effect. It also can aide in finding ways out.

Technical Overview of Basic Filters

Firewalls are used to block Ports. TCP, UDP, ICMP, etc.
OSI Layer 4

Access Control Lists are used to block Routes.
OSI Layer 3

Easy to impliment as well powerful.

Technical Overview of Basic Filters

SIP vs. IAX

Default Ports:

SIP => UDP+TCP 5060 + sometimes 10k – 20k UDP ports?!? Quite easy for a firewall notice.

IAX => UDP 4569 – One Port! Easily transportable on any port.

Which would be easier for a firewall to block?

Technical Overview of Basic Filters

The IAX2 IAX Control Poke packet allows for the unauthenticated detection of a running IAX2. This is the primary means to determine if one can gain connectivity to an Asterisk VoIP server.

Once a Poke connection is successful, one could connect to that host with, presumably, **only** a user name and password.

Technical Overview of Basic Filters

The IAX2 IAX Control Poke packet allows for the unauthenticated detection of a running IAX2. This is the primary means to determine if one can gain connectivity to an Asterisk VoIP server.

Once a Poke connection is successful, one could connect to that host with, presumably, **only** a user name and password.

Technical Overview of Basic Filters

Asterisk can only run IAX on a single port.

Asterisk providers whom want to ensure VoIP services can simply implement a specific addition to their Iptables firewall configuration.

Simply take multiple destination UDP port connections and NAT those packets onto the default Asterisk port of UDP 4569.

Technical Overview of Basic Filters

Basic scan:

`./iaxPingPoker.pl -h 127.0.0.1 -sp 1 -dp 1024`

This will scan the IP address of 127.0.0.1 from UDP port 1 through 1024. When it receives a reply, its response is displayed.

Technical Overview of Basic Filters

IP Range Scan:

`./iaxPingPoker.pl -h 192.168.1.0/24`

This will scan the IP range from 192.168.0.1 through 192.168.1.254 on the default port of UDP 4569.

Technical Overview of Basic Filters

DoS Potential:

`./iaxPingPoker.pl -h 127.0.0.1 --dos`

This will connect to IP address 127.0.0.1 and will repeatability poke the server. Considering that there is no network latency on the loopback interface, running this scan causes as interesting result. Running on the same computer, the CPU usage of the script is roughly 10% while Asterisk uses up to 90%!!

To deepen the issue, Asterisk, by default, does not log IAX Poke requests.

Technical Overview of Basic Filters

Injection Technique:

If an attacker were to run the following onto a scanning host

`./iaxPingPoker.pl -h 127.0.0.1 –-inject`

it will produce false positives, This is thanks to forged response packet onto the ip address of 127.0.0.1. Although there are a few additional conditions for this to work, the effect is still obvious.

Autonomously Bypassing VoIP Filters With Asterisk: Let Freedom Ring

The script will be available on securityscraper.com.

Q&A