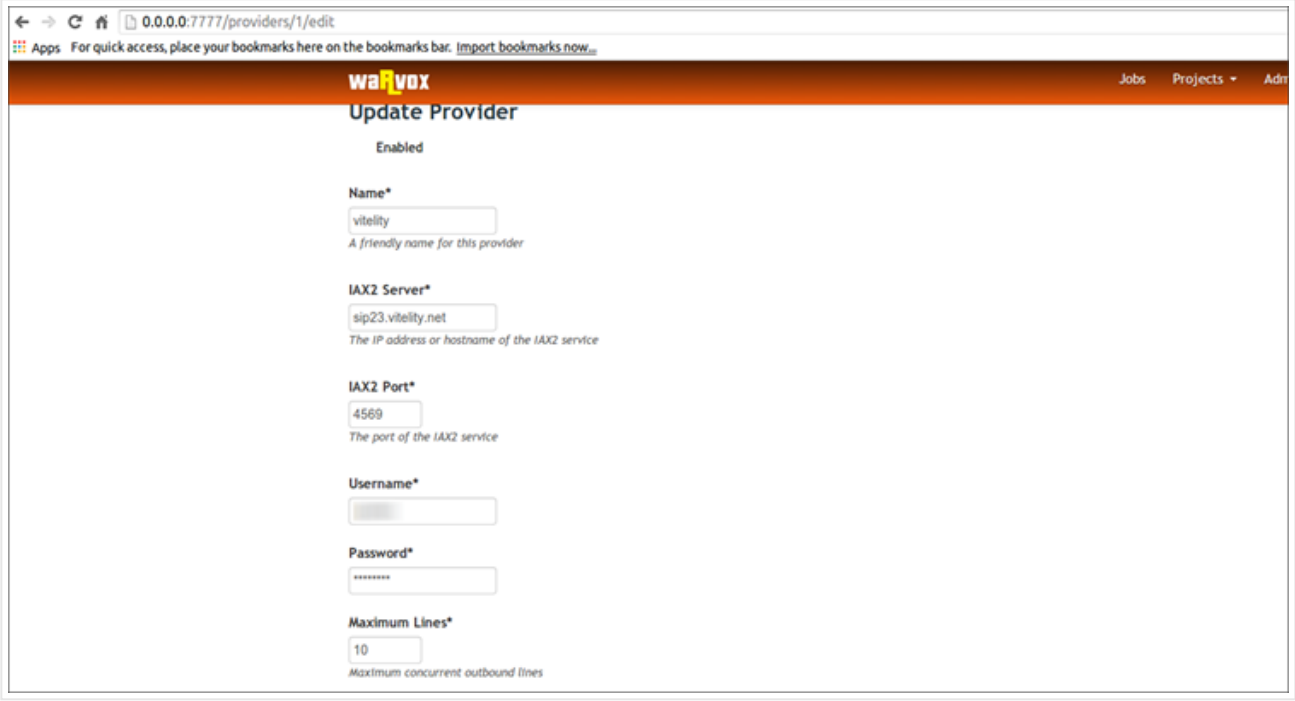
WarVOX Download – War Dialing Tool Software

Last updated: October 18, 2017 | 39,483 views

WarVOX is a suite of tools for exploring, classifying, and auditing telephone systems. Unlike normal wardialing tools, it works with the actual audio from each call and does not use a modem directly.



This model allows the tool to find and classify a wide range of interesting lines, including modems, faxes, voice mail boxes, PBXs, loops, dial tones, IVRs, and forwarders. It provides the unique ability to

What does WarVOX War Dialing Tool Software Do?

WarVOX requires no telephony hardware and is massively scalable by leveraging Internet-based VoIP providers. A single instance on a residential broadband connection, with a typical VoIP account, can scan over 1,000 numbers per hour. The speed is limited only by downstream bandwidth and the limitations of the VoIP service. Using two providers with over 40 concurrent lines we have been able to scan entire 10,000 number prefixes within 3 hours.

WarVOX War Dialing Tools Features

- License changed to BSD, no restrictions on commercial use
- Support number exclusion lists / black lists (regex based)
- Support for phone number ranges in addition to masks
- Support for multiple ranges and masks per job
- Numerous bug fixes and stability improvements
- Command line script for exporting dial results (bin/export_list.rb)

The resulting call audio can be used to extract a list of modems that can be fed into a standard modem-based wardialing application for fingerprinting and banner collection. One of the great things about the WarVOX model is that once the data has been gathered, it is archived and available for re-analysis as new signatures, plugins, and tools are developed. The current release of WarVOX (1.0.0) is able to automatically detect modems, faxes, silence, voice mail boxes, dial tones, and voices.

It is written in Ruby and designed to be run on any modern Linux distribution.

It was actually merged into the Metasploit Project in August 2011.

WarVOX download here:

warvox-master.zip

Or read more here.

Posted in: Hacking Tools

ror, **ruby**, **ruby on rails**, **wardialing**

OWASP APICheck – HTTP API DevSecOps Toolset

APICheck is an HTTP API DevSecOps toolset, it integrates existing tools, creates execution chains easily and is designed for integration with 3rd parties.

October 13, 2020 - 79 Shares

trident – Automated Password Spraying Tool

The Trident project is an automated password spraying tool developed to be deployed on multiple cloud providers and provides advanced options around scheduling

October 7, 2020 - 68 Shares

tko-subs – Detect & Takeover Subdomains With Dead DNS Records

tko-subs is a tool that helps you to detect & takeover subdomains with dead DNS records, this could be dangling CNAMEs point to hosting services and more.

September 24, 2020 - 113 Shares

Arcane – Tool To Backdoor iOS Packages (iPhone ARM)

Arcane is a simple script tool to backdoor iOS packages (iPhone ARM) and create the necessary resources for APT repositories.

August 17, 2020 - 239 Shares

SharpHose – Asynchronous Password Spraying Tool

SharpHose is an asynchronous password spraying tool in C# for Windows environments that takes into consideration fine-grained password policies and can be run over Cobalt Strike's execute-assembly.

July 27, 2020 - 247 Shares

Axiom – Pen-Testing Server For Collecting Bug Bounties

Project Axiom is a set of utilities for managing a small dynamic infrastructure setup for bug bounty, basically a pen-testing server out of the box with 1-line.

July 7, 2020 - 361 Shares

‹ Obama To Create Cyber Security Czar In White House

Hackers Exploiting Unpatched DirectX Bug With Quicktime ›

6 Responses to *WarVOX Download – War Dialing Tool Software*

is wardialling really still really as important as it was a decade or two ago?? I mean I do know tht many greats started off with stuff like wardialling, but whts really the use of a traditional wardialling in todays scenario of high speed broadband internet??

please someone clarify……sorry if this seems like a n00b question

Bogwitch May 28, 2009 at 11:52 am #

Hi Navin,

You're right to say it's not as relevant today as it may have been in the past however, there are still some legacy systems that are connected via modems, some 'emergency access' points, some network infrastructure and some SCADA stuff.
The ability to detect PBX, voicemail etc gives an additional avenue where social engineering can be exploited, too.

send9 May 28, 2009 at 4:55 pm #

Navin: It's important for many of the reasons you stated. People secure their Internet-facing hosts, but forget about their back-up dial-in modems. Vendors will come in and put a modem on their router/equipment/HVAC system for maintenance purpose without telling the organization, as well. Oftentimes the organization is lulled into a false sense of security, without being aware that this threat exists. They will perform their own security audits, but will not include their dial-in lines. It's just an area that's often missed, and one where pen-testers will often have a finding, whereas everything else is in perfect shape. Is it as important as a decade ago? Probably not. But it's certainly very important.

And to add to that, there's not a whole lot of good war dialing software on the market. There are the classics like THCScan and ToneLoc, but they don't perform a whole lot in the way of intelligent detection of carriers and just don't scale well for modern environments or larger pen-tests. And then there's Sandstorm's PhoneSweep, which is buggy and expensive. So to see something like WarVOX, with its new approach and focus on using VoIP, is pretty exciting.

annon June 5, 2009 at 1:37 am #

ok my question is: is this legal? because i see it just as war driving only by using ur dial up modem as the "beacon"… thing is i have heard that after the "phone phreaking" age implementations were put in so users could not war dial and if they were caught doing so they might be punished to the full extent of the law!?! am i wrong in saying this might be gray area sofware? I would like to know seeing as how im interested…

Bogwitch June 5, 2009 at 3:07 pm #

As with all forms of penetration testing, without the system owner's permission would be illegal (in most contries)

If you try to run a war-dialler without permission from the target owner, expect to get v&

erleko July 1, 2009 at 10:17 pm #

ye s you will be caught and prosectued.

Search Darknet

Search...

TRENDING LATEST POSTS

tko-subs – Detect & Takeover Subdomains With Dead DNS Records
SEPTEMBER 24, 2020 - 113 SHARES

OWASP APICheck – HTTP API DevSecOps Toolset
OCTOBER 13, 2020 - 79 SHARES

trident – Automated Password Spraying Tool
OCTOBER 7, 2020 - 68 SHARES

Advertisements

Topics

Advertorial (36)

- Database Hacking (89)
- Events/Cons (7)
- Exploits/Vulnerabilities (429)
- Forensics (64)
- Hacker Culture (8)
- Hacking News (235)
- Hacking Tools (671)
- Hardware Hacking (82)
- Legal Issues (179)
- Linux Hacking (72)
- Malware (238)
- Networking Hacking Tools (351)
- Password Cracking Tools (105)
- Phishing (41)
- Privacy (217)
- Secure Coding (119)
- Security Software (229)
- Site News (51)
  - Authors (6)
- Social Engineering (36)
- Spammers & Scammers (76)
- Stupid E-mails (6)
- Telecomms Hacking (6)
- UNIX Hacking (6)
- Virology (6)
- Web Hacking (384)
- Windows Hacking (169)
- Wireless Hacking (45)

Privacy Policy