- Home
- About
- Archive
- Contact

Menu

SecTechno
Information Security Blog

- News
- Malwares
- Tools
- Vulnerabilities
- Open-Source
- Pentesting
- Cybercrime & Hacking
- Web Security
- Cloud Computing

Navigation

January 31, 2016 Open-Source, Tools 0 Comments

Beurk – Experimental Unix Rootkit

Hello fellow Twitter user! Don't forget to Twit this post if you like it, or follow me on Twitter if you find me interesting.

BEURK is a userland preload rootkit for GNU/Linux, heavily focused around anti-debugging and anti-detection. the tool can be used during a penetration testing to hide files and directories on targeted system, it will also allow to detect user login and access on the system and collect credentials, This beside use it as a backdoor on the system to remotely open a remote session and take control on the system.

Some of the features are:

- Hide attacker files and directories
- Realtime log cleanup (on utmp/wtmp)
- Anti process and login detection
- Bypass unhide, lsof, ps, ldd, netstat analysis
- Furtive PTY backdoor client

Author is planning to add more features for the upcoming releases:

- ptrace hooking for anti-debugging
- libpcap hooking undermines local sniffers
- PAM backdoor for *local privilege escalation*

Usage and to Compile the package do the following:

```
git clone https://github.com/unix-thrust/beurk.git
cd beurk
make Install
```

You can download this tool over this link: https://github.com/unix-thrust/

- CANard – Vehicle Hacking Platform
- Keep Your Unix-Based System Safe This Summer (Part2)

- GCAT – Fully featured backdoor that uses Gmail as a C&C server
- Lynis v2.0.0- Security auditing and hardening tool

Share / Save

Beurk, Hacking tool, open source, Rootkit, UNIX

0 Comments SecTechno 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Add Disqus Add Privacy DISQUS

- Follow Us!
- Recent Posts
  - Beurk – Experimental Unix Rootkit
  - Network & Data Isolation: Can It Keep Your Company’ s Cloud Secure?
  - Maltrail – Malicious traffic detection system
  - ISP-SEC – Cyber Threat Intelligence Platform
  - HSBC Customers Targeted with Phishing Scam
- Blogroll
  - Brian Honan Blog
  - Didier Stevens
  - Fortalice
  - Infosec Ramblings
  - J4VV4D Blog
  - SANS Blog
  - The New School of Information Security
  - The Roer.com Information Security Blog
- Search