GoldenEye Release Candidate 1

written by mæÐmå×
11/01/2000
>>current version 1.0.5.120<<

This program is freeware and may not be sold!

- Legal disclaimer
  ==========

GoldenEye is a brute-force hacking program and was written for web-masters to test the of their own sites.
It should not be use by others to hack sites - this would be illegal!
In no event, the author or any other persons involed in its development will be held liable for the misuse of the program.

- A few notes:
  ==========

- GoldenEye works with different types of wordlists:

"username:password", "username [TAB] password" or single lists (normal mode or iterative mode)

- GoldenEye executes its attempts simultaneously. The number of simultanous attempts can be adjusted
with the speed slider on the "access" tab. You can also adjust the speed limit. On the Options|Connections tab
you'll find a box to set the "top-speed"; select an apropiate value. Use lower values for slow internet connection!
If you get to much timed-out connections, lower the crack speed or increase the TTL (time to life). Timed-out
connections will be automatically resumed if you check 'Resume time-out connections automatically' on the same tab.

If you experience ”no buffer space” error messages lower the crack speed and close other programs.

- GoldenEye logs the cracked sites. They are listed on the History|Access History tab.
You can select and delete single entries or the whole list. Expired combinations will be automatically removed
when you click the check for expired passwords button. Click on the 'visit button' or double click on the selected url
to launch it in your browser.

Notes for single pass cracks: The shipped presets are examples. Please use your own values.

- Options|Advanced tab:

* Change proxy after x attempts. GoldenEye changes the proxy automatically after x attempts if this options is checked.
You have to use several proxies to use this feature. Add proxies on the Options|

connections tab.
GoldenEye changes the proxy randomly or in the order which is given by the proxy-list.
* Server Response: the standard values are '200' for ok and '401' for access denied (unauthorized). If the server you're attacking
gives other reply numbers you can change them. Note: You can't use 404 or 500!
* Cookie: If the attacked server needs a cookie, check this option and enter the cookie string.
* Referer: If the attacked server needs the url of the refering site, enter it here.

- Wordlist tools tab

* Remove dups: New: If you're using single lists for userID and password GoldenEye removes the dups simultanous.
* General wordlist options:
Define a mininum and maximum length for the userID and password (standard settings 1-32)
Convert the list: All passes will be converted 'on-the-fly'.
Wordlist style: If you want to use single lists: check this option.
* Wordlist manipulations: this tab appears after you've loaded a list and checked the 'Extend list' on "General wordlist"
"Common manipulations" are predefined manipulations.
On the "Advanced" tab you can choose your own prefixes, suffixes, etc. If you miss something, tell me!

- Security check

* Server security test: It tests the attacked server for other security holes.
* Proxy test: tests the proxy-speed. The values are in milliseconds.

Version history:

==========

- Version 1 beta: (06/99)
I found several security tools on the internet. All of them processed the attempts sequentially.
This one-by-one method was quiet slow and so I ran several instances with small wordlists each.
Because it was very complicated to load the lists and enter the URL in each instance of the program I decided to write a program which does that automatically.
Very soon after I've started to code my own program Claudio Destito published HackerTTP which
did the same job and so I've stopped my work. But after I wanted to download a newer version
(~3 MB) and the connection broke down on each attempt I returned to my own code and adopted
the functions and the user-interface from HackerTTP (I have great respect for 'Claudio' and his program).

- Version 1 beta 2: (07/99)
* rewrote complete source code
* some bug-fixes
* added iterative single list use
* added user-agent, TTL and a proxy-list property
* new design: pagecontrol instead of seperate windows

- Version 1 beta 2.1 (07/99)

  * added some a tool for on-the-fly wordlist manipulation
  * removed some bugs

- Version 1 beta 3
  * changed the design
  * some bug-fixes
  * added a proxy speed test
  * added some further options
  * added a change proxy feature

- Version 1 release candidate 1
 * some bug-fixes
 * new access and url history
 * more options
 * list queues
 * autopilot
 * backdoor scan
 * support for own exploit lists

- Version 1 release candidate 2
 * some bug-fixes
 * new file format for access history
 * single pass and html crack feature
 * proxy-tester
 * more options

Special thanks to PhÖßetøR for joining the project.

Many thanks to all beta-testers!

PLEASE NOTE: This program is distributed without warranties to be bug-free.
Some virus-scanner give false alarms (win32 virus) because of the exe-code compression
used to make GoldenEye smaller in size. There's is NO malicious code - NO virus - NO trojan in
GoldenEye!

If you find any bugs or have comments, ideas or suggestions please let me know.
The more the better! GoldenEye gets a better tool with your feedback.

Please don't email requests for wordlists, hacking sites, etc.

madmax98@hotmail.com