



Goohack

Information Security Inc.

Contents

- About Goohack
- Testing Environment
- Required packages
- Installing Goohack
- Using Goohack
- References

About Goohack

- GooHak is a shell script to automatically launch google hacking queries against a target domain to find vulnerabilities and enumerate a target

GooHak v1.6 by 1N3@CrowdShield

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Required packages

- iceweasel

```
root@kali2017:~# apt-get install iceweasel  
Reading package lists... Done  
Building dependency tree
```

Installing Gohack

- Download GitHub repository

```
root@kali2017:~# git clone https://github.com/1N3/Goohak.git
Cloning into 'Goohak'...
remote: Counting objects: 59, done.
remote: Total 59 (delta 0), reused 0 (delta 0), pack-reused 59
Unpacking objects: 100% (59/59), done.
```

Installing Gohack

- goohak script

```
root@kali:~# cat goohak
#!/bin/bash
# + -- ==[GooHak by IN3
# | -- == [http://crowdshield.com
#
# ABOUT:
# GooHak is a shell script to automatically launch google hacking queries against a target domain to find vulnerabilities and enumerate a target.
#
# DEPENDENCIES:
# iceweasel or xdg-utils (apt-get install xdg-utils)
# Linux
#
TARGET="$1"
BROWSER="iceweasel" # CHANGE TO DEFAULT BROWSER OR USE iceweasel
VER="1.7"
OKBLUE='\033|94m'
OKRED='\033|91m'
OKGREEN='\033|92m'
OKORANGE='\033|93m'
RESET='\033|0m'

if [ -z $TARGET ]; then
    echo -e "$OKORANGE + -- ==[http://crowdshield.com$RESET"
    echo -e "$OKORANGE | -- == [GooHak v$VER by IN3$RESET"
    echo -e "$OKORANGE + -- ==[Usage: goohak <domain>$RESET"
    exit
fi

$BROWSER 2> /dev/null &
sleep 5

# LOAD WEBSITE IN A WEB BROWSER
$BROWSER http://$TARGET 2> /dev/null
$BROWSER https://$TARGET 2> /dev/null
# TCPIPUTILS
$BROWSER http://www.tciputils.com/browse/domain/$TARGET 2> /dev/null
# NKTCRAPT
$BROWSER http://toolbar.netcraft.com/site_report?url=$TARGET 2> /dev/null
# SHODAN
$BROWSER https://www.shodan.io/search?query=$TARGET 2> /dev/null
# CENSYS
$BROWSER https://www.censys.io/ipv4?q=$TARGET 2> /dev/null
# CRT.SH
$BROWSER https://cert.sh/?q=%25.$TARGET 2> /dev/null
# ZONE-H
$BROWSER "https://www.google.ca/search?q=site:zone-h.org:$TARGET" 2> /dev/null
# XSSPOSED
$BROWSER "https://www.xsposed.org/search/?search=$TARGET&type=host" 2> /dev/null
```

Using Goohack

- Running Goohak

```
root@kali2017:~# cd Goohak/  
root@kali2017:~/Goohak# ./goohak  
+ -- ==[http://crowdshield.com  
+ -- ==[GooHak v1.7 by 1N3  
+ -- ==[Usage: goohak <domain>
```


Using Goohack

- Running Goohack => Netcraft

```
root@kali2017:~/Goohack# ./goohak isec.ne.jp
```



Site report for isec.ne.jp

Search... →

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Donations

Lookup another URL: Enter a URL here

Share: [f](#) [t](#) [in](#) [g+](#) [v](#) [p](#)

Background

Site title	サイバーセキュリティ対策 情報セキュリティ株式会社	Date first seen	December 2014
Site rank		Primary language	Japanese

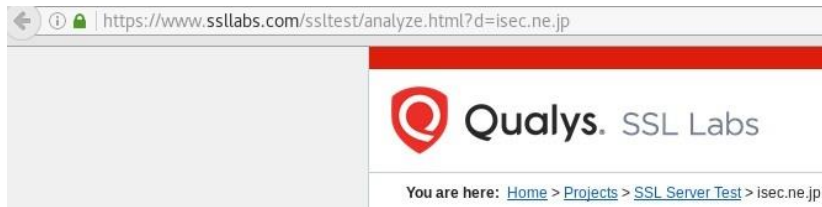
Using Goohack

- Running Goohak => Shodan



Using Goohack

- Running Goohak => SSL Labs



References

- Howucan
<https://howucan.gr/scripts-tools/2134-goohak-automatically-launch-google-hacking-queries-against-a-target-domain>
- Kali Linux
<https://www.kali.org/downloads/>
- Shodan
<https://www.shodan.io/>