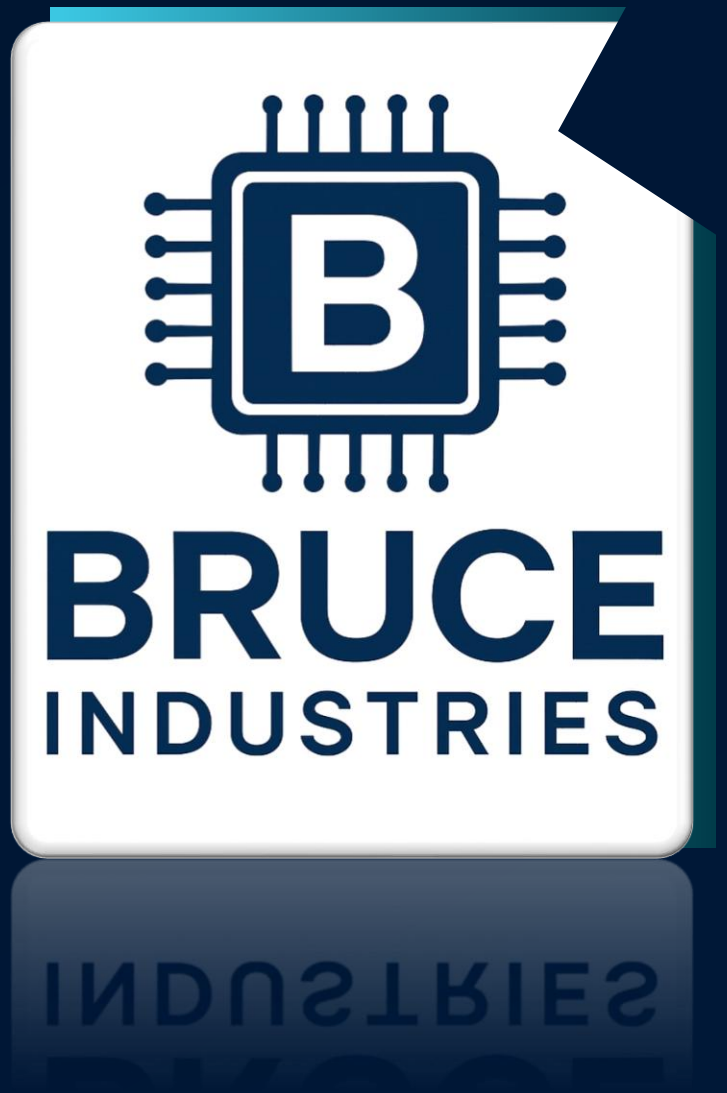
Bruce Industries: Incident Response Focusing on Digital Forensics

Organization Background



Bruce Industries:

- A globally recognized and leading VLSI (Very-Large-Scale Integration) design and semiconductor manufacturing firm.
- With decades of innovation and excellence, the company specializes in evolving proprietary chip blueprints and pioneering microarchitecture designs.
- Serve as the advancements for next-generation of computing technologies.

To fight with the increasing threat of cyber-espionage and sensitive assets, company implemented TLS system also known as SSL proxy to inspect internal HTTPS traffic for some malware or data exfiltration.

Incident Overview

Internal monitoring systems flagged unusual activity originating from a server used by the HR department.

The system was known to handle encrypted archives containing sensitive employee information.

The nature of the alerts prompted the security team to escalate the issue to Incident Response and Digital Forensics teams.

No immediate external breach was confirmed, but early signs warranted a closer look.

Incident Response Planning

- **Identify** and confirm the security incident
- **Contain** the threat to prevent further damage
- **Eradicate** malicious activity from affected systems
- **Recover** systems and resume normal operations
- **Learn** from the incident to improve future defenses

Here we're focusing more on Forensics side

Containment

- **Containment** is the process of **limiting the impact** of a security incident before it spreads further.

Disconnecting a compromised device from the network.

- Blocking malicious IP addresses or domains.
- Disabling user accounts such as HR account and IT admin of that machine.
- Redirecting traffic or changing firewall rules.

Observed Exploitation Pattern

Initial access was gained through a web-based vulnerability introduced into the HR portal.

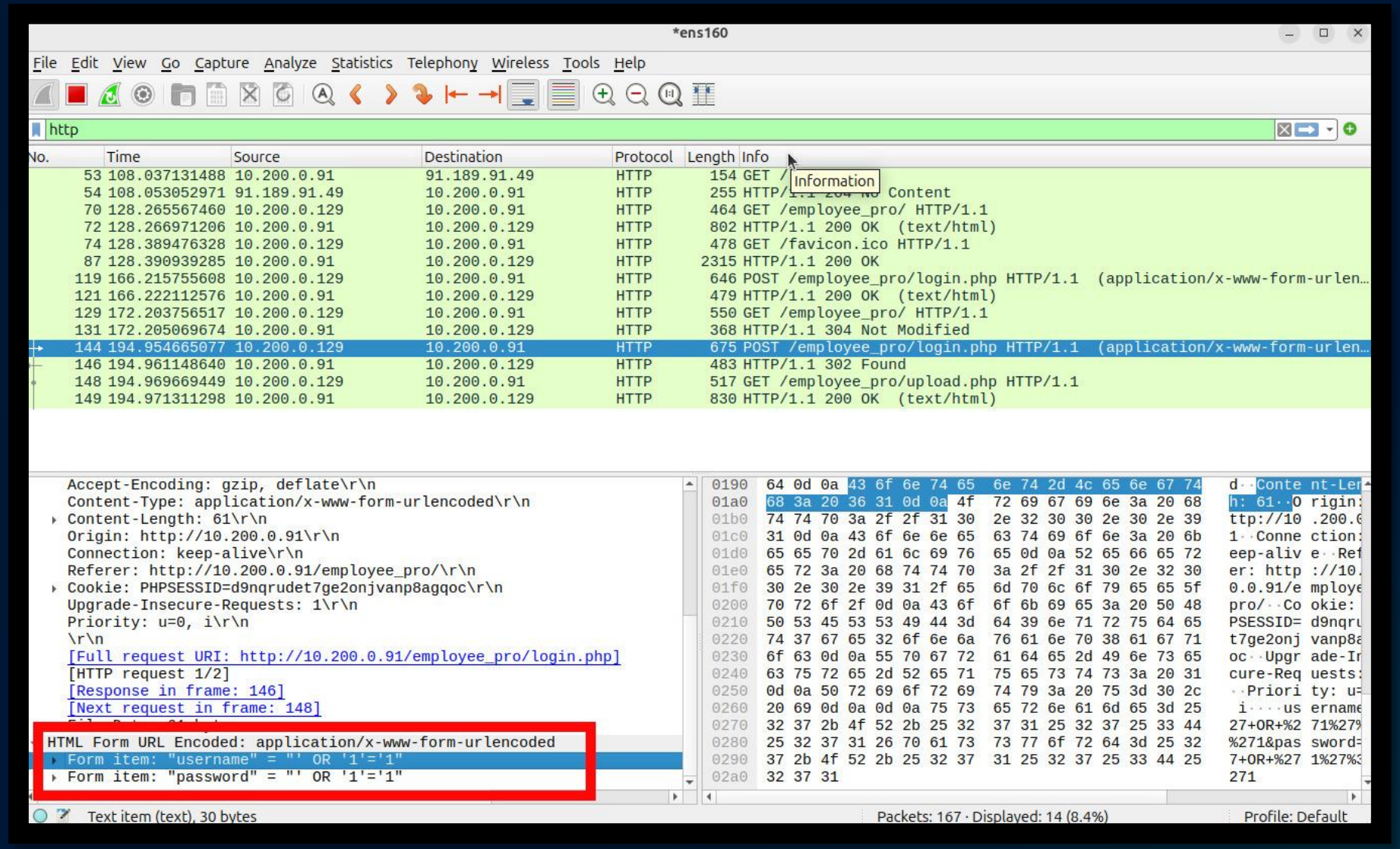
The attacker escalated privileges using misconfigured local permissions and accessed sensitive directories.

Final actions involved data exfiltration through a covert channel, bypassing traditional alerting mechanisms.

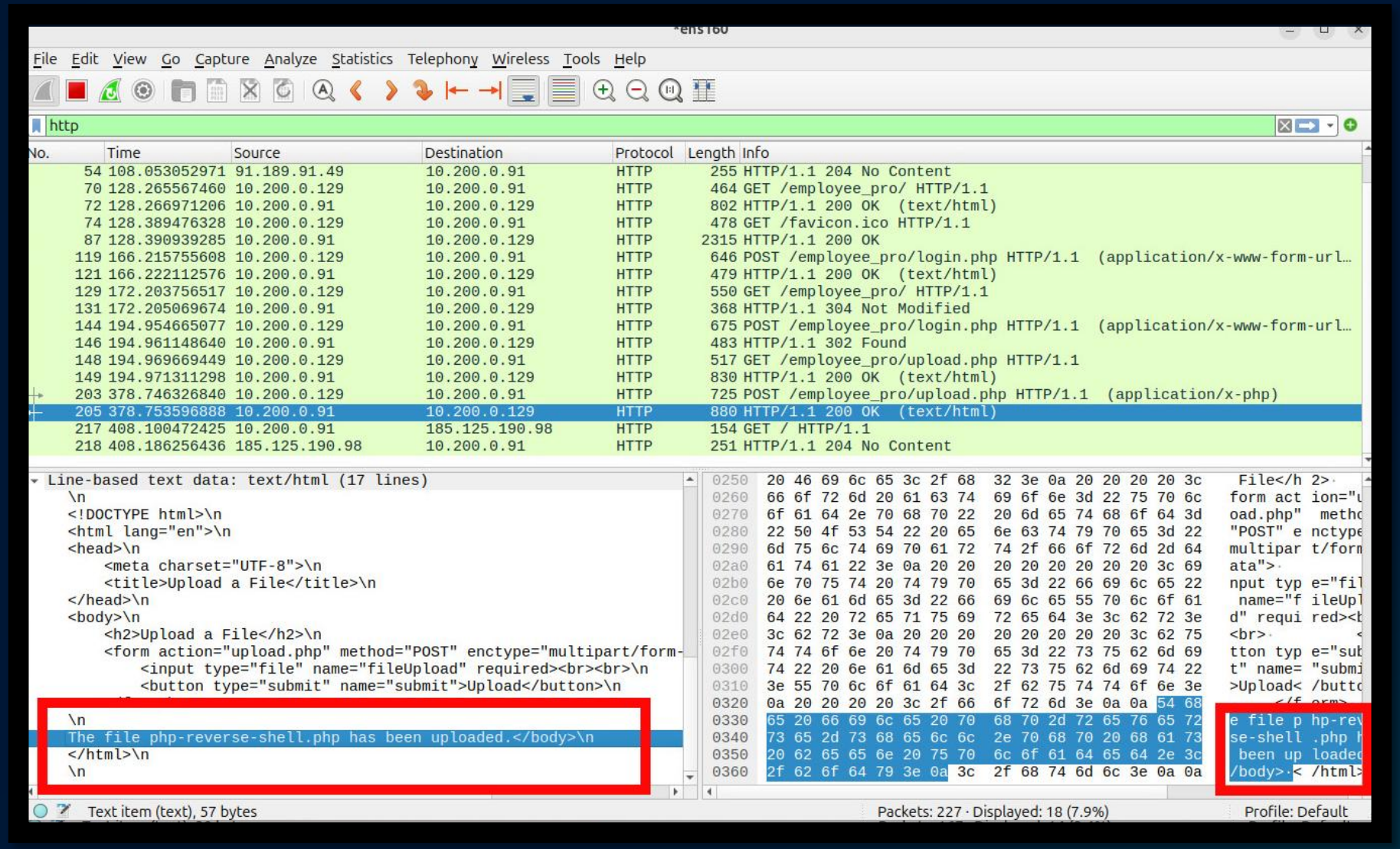
Packet captures and protocol analysis provided step-by-step evidence of the entire attack flow.

The investigation uncovered a multi-step exploitation process, each action building on the previous one.

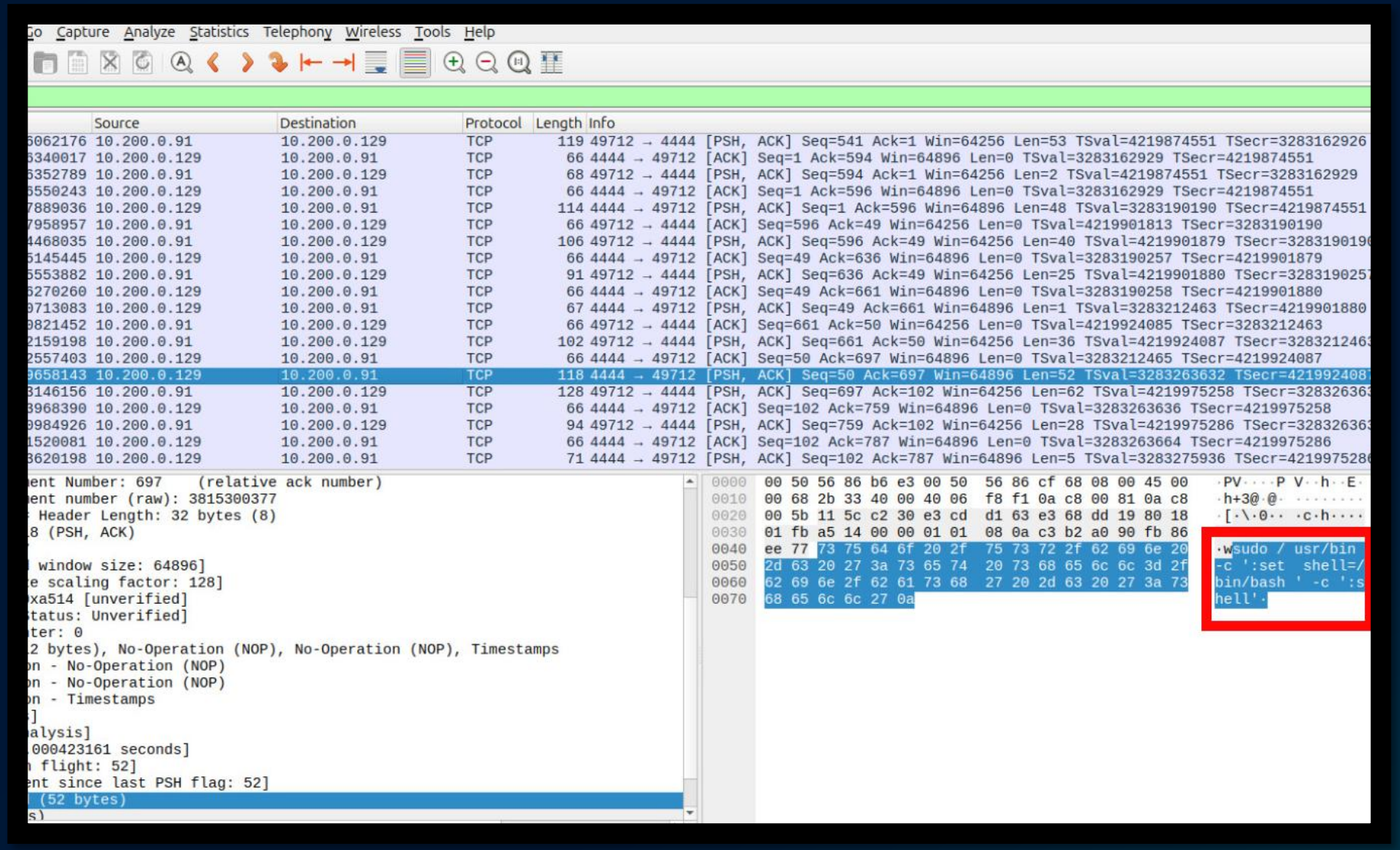
SQL Injection



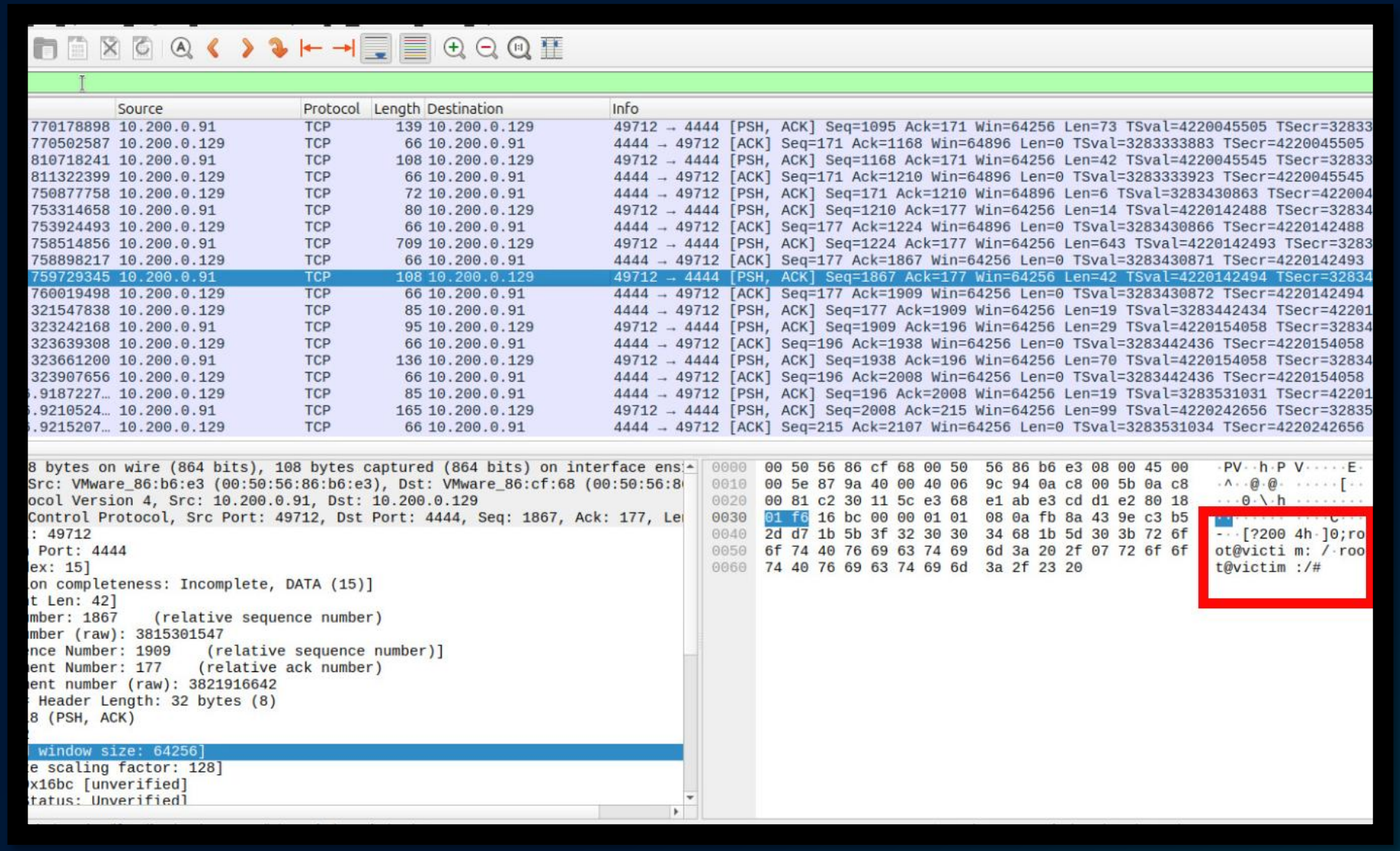
RFI File Upload



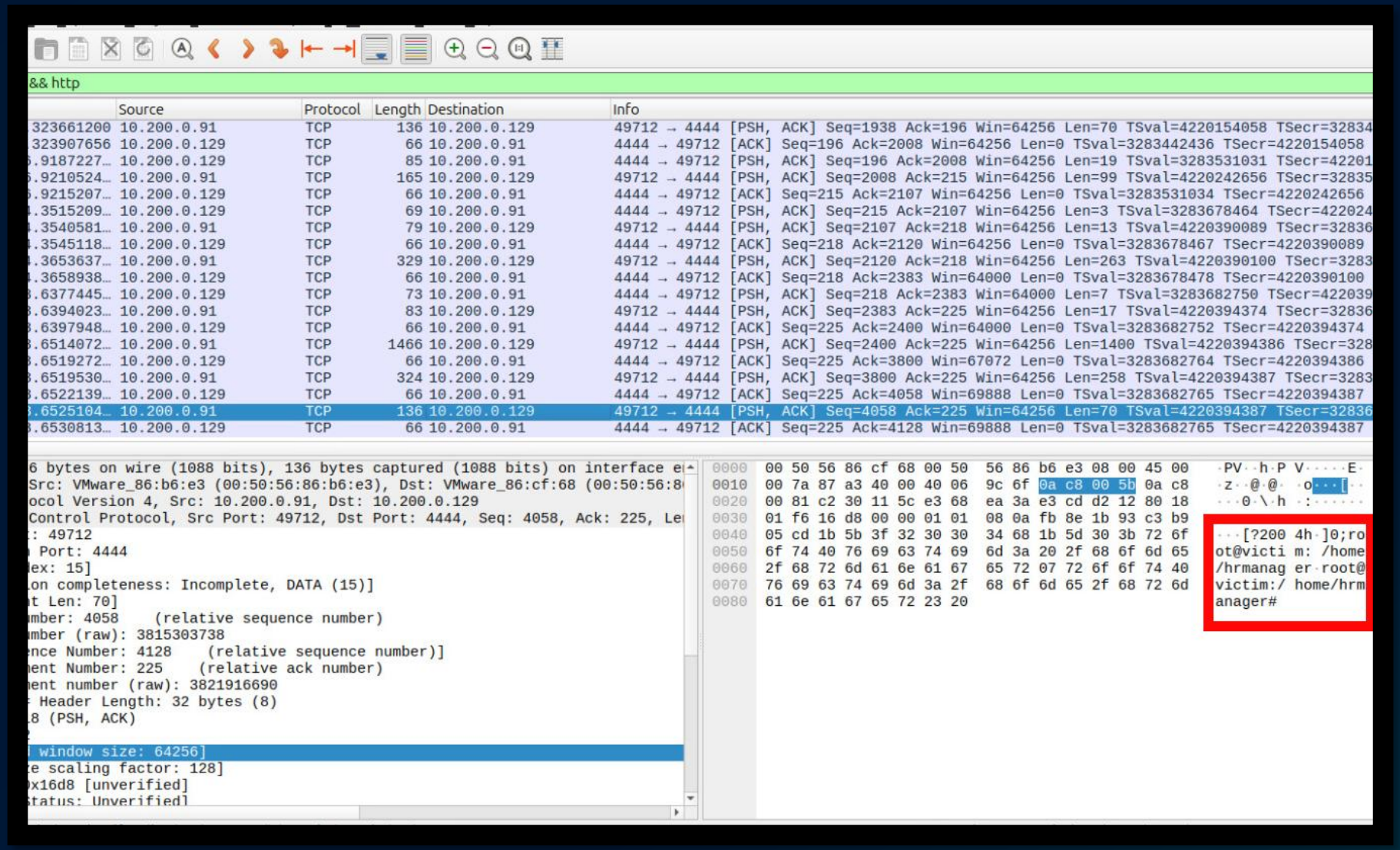
Exploiting VIM sudo vulnerability



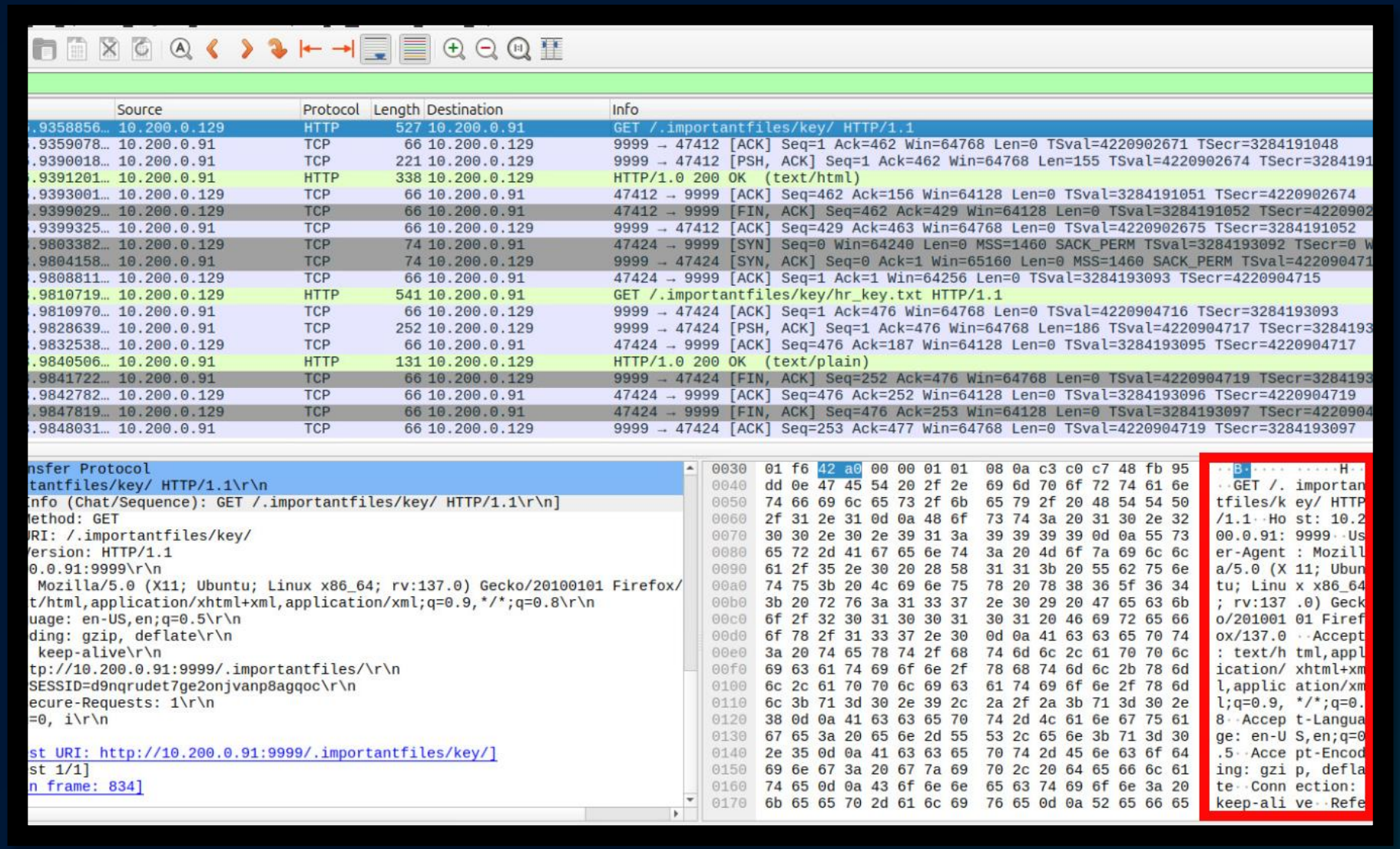
Root Access at Victim Machine



Attacker Reconnaissance Within HR Directory



Attacker exfiltrating data through Python Server



	Source	Protocol	Length	Destination	Info
.9358856…	10.200.0.129	HTTP	527	10.200.0.91	GET /.importantfiles/key/ HTTP/1.1
.9359078…	10.200.0.91	TCP	66	10.200.0.129	9999 → 47412 [ACK] Seq=1 Ack=462 Win=64768 Len=0 TSval=4220902671 TSecr=3284191048
.9390018…	10.200.0.91	TCP	221	10.200.0.129	9999 → 47412 [PSH, ACK] Seq=1 Ack=462 Win=64768 Len=155 TSval=4220902674 TSecr=3284191
.9391201…	10.200.0.91	HTTP	338	10.200.0.129	HTTP/1.0 200 OK (text/html)
.9393001…	10.200.0.129	TCP	66	10.200.0.91	47412 → 9999 [ACK] Seq=462 Ack=156 Win=64128 Len=0 TSval=3284191051 TSecr=4220902674
.9399029…	10.200.0.129	TCP	66	10.200.0.91	47412 → 9999 [FIN, ACK] Seq=462 Ack=429 Win=64128 Len=0 TSval=3284191052 TSecr=4220902
.9399325…	10.200.0.91	TCP	66	10.200.0.129	9999 → 47412 [ACK] Seq=429 Ack=463 Win=64768 Len=0 TSval=4220902675 TSecr=3284191052
.9803382…	10.200.0.129	TCP	74	10.200.0.91	47424 → 9999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3284193092 TSecr=0 W
.9804158…	10.200.0.91	TCP	74	10.200.0.129	9999 → 47424 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=422090471
.9808811…	10.200.0.129	TCP	66	10.200.0.91	47424 → 9999 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3284193093 TSecr=4220904715
.9810719…	10.200.0.129	HTTP	541	10.200.0.91	GET /.importantfiles/key/hr_key.txt HTTP/1.1
.9810970…	10.200.0.91	TCP	66	10.200.0.129	9999 → 47424 [ACK] Seq=1 Ack=476 Win=64768 Len=0 TSval=4220904716 TSecr=3284193093
.9828639…	10.200.0.91	TCP	252	10.200.0.129	9999 → 47424 [PSH, ACK] Seq=1 Ack=476 Win=64768 Len=186 TSval=4220904717 TSecr=3284193
.9832538…	10.200.0.129	TCP	66	10.200.0.91	47424 → 9999 [ACK] Seq=476 Ack=187 Win=64128 Len=0 TSval=3284193095 TSecr=4220904717
.9840506…	10.200.0.91	HTTP	131	10.200.0.129	HTTP/1.0 200 OK (text/plain)
.9841722…	10.200.0.91	TCP	66	10.200.0.129	9999 → 47424 [FIN, ACK] Seq=252 Ack=476 Win=64768 Len=0 TSval=4220904719 TSecr=3284193
.9842782…	10.200.0.129	TCP	66	10.200.0.91	47424 → 9999 [ACK] Seq=476 Ack=252 Win=64128 Len=0 TSval=3284193096 TSecr=4220904719
.9847819…	10.200.0.129	TCP	66	10.200.0.91	47424 → 9999 [FIN, ACK] Seq=476 Ack=253 Win=64128 Len=0 TSval=3284193097 TSecr=4220904
.9848031…	10.200.0.91	TCP	66	10.200.0.129	9999 → 47424 [ACK] Seq=253 Ack=477 Win=64768 Len=0 TSval=4220904719 TSecr=3284193097

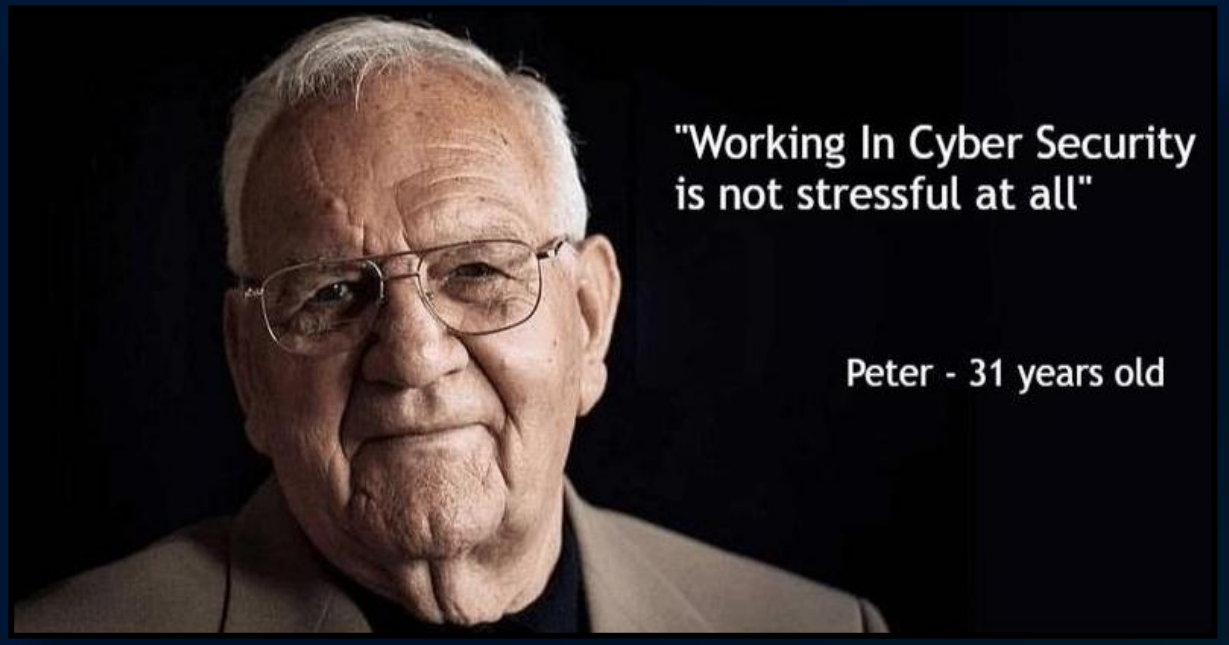
```
nsfer Protocol
tantfiles/key/ HTTP/1.1\r\n
nfo (Chat/Sequence): GET /.importantfiles/key/ HTTP/1.1\r\n]
ethod: GET
RI: /.importantfiles/key/
ersion: HTTP/1.1
0.0.91:9999\r\n
 Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/
t/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
uage: en-US,en;q=0.5\r\n
ding: gzip, deflate\r\n
 keep-alive\r\n
tp://10.200.0.91:9999/.importantfiles/\r\n
SESSID=d9nqrudet7ge2onjvanp8agqoc\r\n
ecure-Requests: 1\r\n
=0, i\r\n

st URI: http://10.200.0.91:9999/.importantfiles/key/]
st 1/1]
n frame: 834]
```

```
0030  01 f6 42 a0 00 00 01 01  08 0a c3 c0 c7 48 fb 95   ··B·····  ·····H··
0040  dd 0e 47 45 54 20 2f 2e  69 6d 70 6f 72 74 61 6e   ··GET /. importan
0050  74 66 69 6c 65 73 2f 6b  65 79 2f 20 48 54 54 50   tfiles/k ey/ HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 30 2e 32   /1.1··Ho st: 10.2
0070  30 30 2e 30 2e 39 31 3a  39 39 39 39 0d 0a 55 73   00.0.91: 9999··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 58  31 31 3b 20 55 62 75 6e   a/5.0 (X 11; Ubun
00a0  74 75 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   tu; Linu x x86_64
00b0  3b 20 72 76 3a 31 33 37  2e 30 29 20 47 65 63 6b   ; rv:137 .0) Geck
00c0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
00d0  6f 78 2f 31 33 37 2e 30  0d 0a 41 63 63 65 70 74   ox/137.0 ··Accept
00e0  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 61 70 70 6c   : text/h tml,appl
00f0  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/ xhtml+xm
0100  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 6d   l,applic ation/xm
0110  6c 3b 71 3d 30 2e 39 2c  2a 2f 2a 3b 71 3d 30 2e   l;q=0.9, */*;q=0.
0120  38 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   8··Accep t-Langua
0130  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0140  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
0150  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0160  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection:
0170  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 52 65 66 65   keep-ali ve··Refe
```

What's Next?

Lessons Learned?

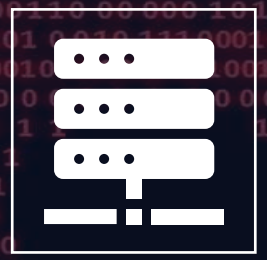
Any Questions?



Peter with data

Red Flags in Vulnerability Pattern

During initial analysis, forensic investigators observed a suspicious pattern



Multiple critical vulnerabilities were present on the same system:

SQL Injection in HR web portal

Remote File Inclusion (RFI) upload capability

Privilege escalation via sudo misconfiguration (vim NOPASSWD for daemon)

This combination felt unusual and intentional, not accidental.

Decision was made to perform deep-dive forensic analysis on the full disk image of the machine to identify potential insider involvement.

Truths are yet to be uncovered...

Steganography techniques found

```
└─$ strings Peter.png
IHDR
IDATx
yzzkF
3&32
f+Rw
3c(8o
'Z_;
:5&q
("  J
1ku~
v$b7
LG^@7
3J7Ee
nlwz
)"! s
*D
^<{
+rZ
Roi
%]&
'xoo
'@:
r};{
);rI@i
Vm+
```

```
┌──(kathir㉿Kali)-[~/Steganography]
└─$ python3 Steganography.py

Steganography found and extracting the message:

Employee ID,Full Name,SSN
EID1023,James Mckenzie,694-22-7813
EID1024,Alexis Knight,106-99-8878
EID1025,Brittany Johnson,159-77-7857
EID1026,Haley Harris,843-12-2686
EID1027,Samantha Savage,136-74-4273
EID1028,Melinda Torres,309-94-4515
EID1029,Emily Watkins,531-93-8018
EID1030,Michele Smith,204-91-3129
EID1031,Sean Petty,552-57-2208
EID1032,Amy Moyer,392-93-2615
EID1033,Jennifer Fleming,290-41-7920
EID1034,Laura Pierce,587-84-2329
EID1035,Katherine Ortiz,402-62-6303
EID1036,Cynthia Marshall,164-35-6683
EID1037,Charles Rivera,835-86-6188
EID1038,Theodore Smith,324-87-4168
EID1039,Vanessa Nguyen,754-51-2792
EID1040,Bobby Wood MD,152-51-8169
EID1041,Scott Garcia,116-86-7795
EID1042,Victor Reilly DVM,830-91-7003
EID1043,Timothy Barron,765-16-1321
```

Steganography techniques found in Faraz directory

While analyzing Faraz's user directory from the disk image

Investigators discovered **suspicious image files**

One image was confirmed to contain **hidden SPII (SSNs and employee data)** using **steganographic techniques**

This immediately raised concern:

Why was sensitive HR data embedded inside media files?

Who had access to both HR data and stego tools?

To confirm **how and when** the data was accessed:

The team began reviewing **authentication logs (/var/log/auth.log)**

Auth log review focused on:

Sudo sessions

User switches (su)

Access timestamps to /home/hrmanager

```
2025-04-15T00:00:57.405323-04:00 victim sudo: hrmanager : TTY=pts/0 ; PWD=/home/hrmanager ; USER=root ; COMMAND=/usr/sbin/usermod -aG sudo faraz
2025-04-15T00:00:57.455370-04:00 victim usermod[47226]: add 'faraz' to group 'sudo'
2025-04-15T00:00:57.456161-04:00 victim usermod[47226]: add 'faraz' to shadow group 'sudo'
```

Privilege escalation

```
2025-04-15T00:33:07.643585-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/ls -a /home/hrmanager/.importantfiles/key
2025-04-15T00:33:07.646674-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:34:27.571117-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/.importantfiles/key/hr_key.t
xt /home/faraz/Documents/interesting.txt
2025-04-15T00:34:27.572997-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:35:44.944016-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents ; USER=root ; COMMAND=/usr/bin/ls -a /home/hrmanager/.importantfiles
/
2025-04-15T00:35:44.947034-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:36:43.828156-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/.importantfiles/ss
h_data.enc /home/faraz/Documents/very_interesting.enc
```

Encryption key extraction

```
2025-04-15T00:43:02.093297-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz ; USER=root ; COMMAND=/usr/bin/cp /home/hrmanager/Documents/.confidential/.sec
ret.tar.xz.gpg /home/faraz/Documents/others
2025-04-15T00:43:02.098157-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:43:53.521806-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/mv .secret.tar.xz.gpg easy.tar
.xz.gpg
```

Encrypted file extraction

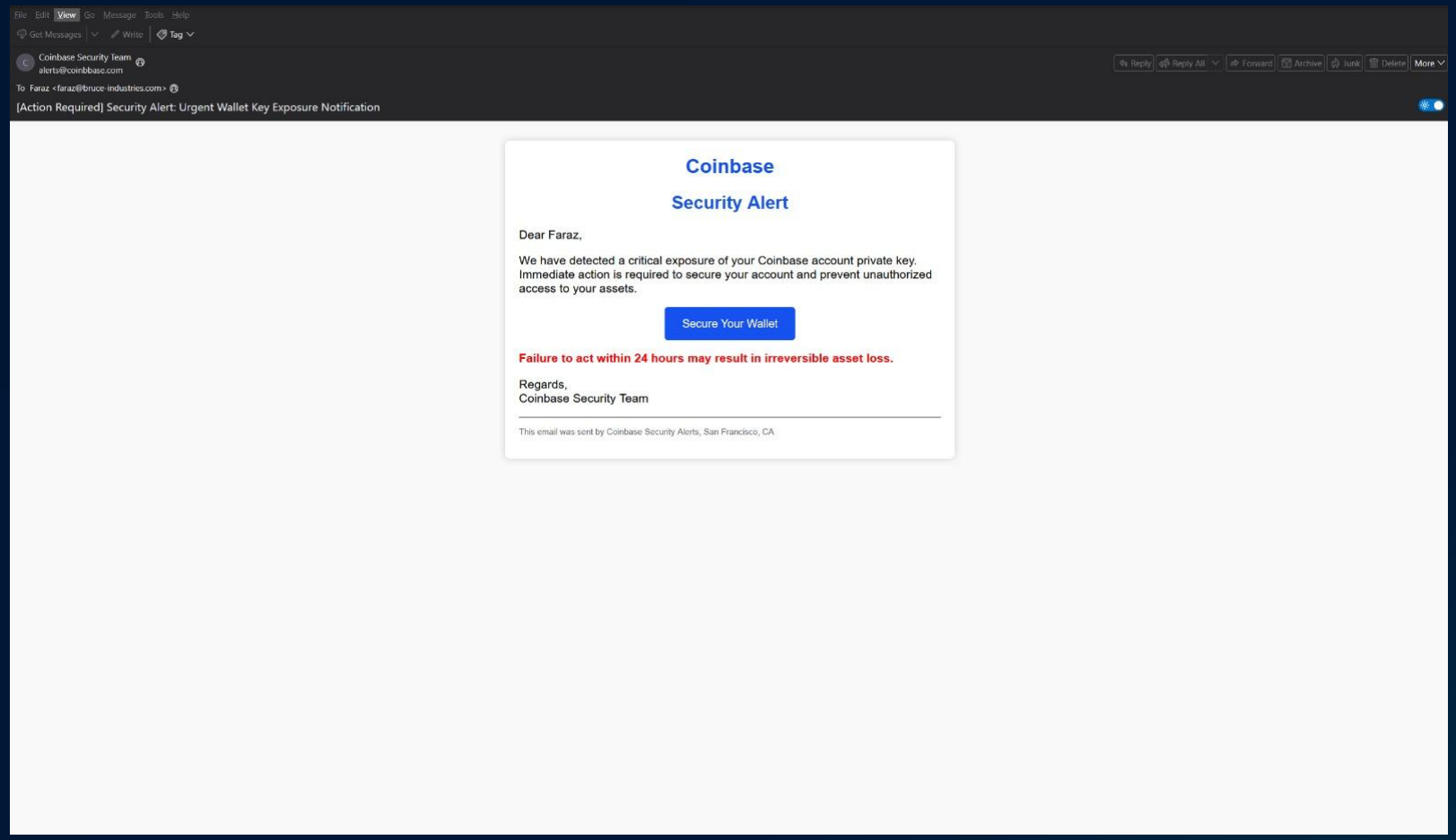
```
2025-04-15T00:55:12.173872-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/cat /home/hrmanager/.local/sha
re/Trash/files/deletethis.txt
2025-04-15T00:55:12.176116-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:55:54.924706-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/gpg --decrypt easy.tar.xz.gpg
2025-04-15T00:55:54.927821-04:00 victim sudo: pam_unix(sudo:session): session opened for user root(uid=0) by faraz(uid=1002)
2025-04-15T00:56:20.202052-04:00 victim sudo:    faraz : TTY=pts/0 ; PWD=/home/faraz/Documents/others ; USER=root ; COMMAND=/usr/bin/gpg --decrypt easy.tar.xz.gpg
```

Decryption

Phishing Email Never reported: A Turning Point in the Case

- During the investigation, a **phishing email** was found in Faraz’s inbox:
- Received from alerts@coinbbase.com (typo squatted domain)
- Posed as a security alert from Coinbase
- **Faraz never reported this email** to the security team
- Contained a **link to a fake website** with threatening instructions to Faraz
- This became a **critical red flag**:
- Showed lack of compliance with phishing awareness protocols
- Suggested **possible cooperation** or intentional negligence
- The email became a **key pivot point** in shifting Faraz's role from victim to potential insider

Initial mail received from Coinbase



The phishing email included a link to: **https://www.coinbbase.com-security-alerts.com/**

To avoid interaction with a live malicious server, the team used a **safe, automated screenshot tool** to analyze the link's destination

The screenshot revealed

A **fake Coinbase-branded webpage**

A threatening message directed at Faraz

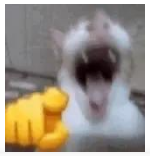
Demands to follow future instructions, including vulnerability injection

This confirmed that the email was part of a **coercive phishing campaign**, contributing to Faraz's compromised behavior

The message for Faraz is

coinbase

Cryptocurrencies Individuals Businesses Institutions Developers Company Sign in Sign up

Hey Faraz, 

I know this is your private key.
[5HueCGU8rMjxEXxiPuD5BDuS7zG1hKRXzjym9ZG7iGJUKz7duDT]
I already transferred **2 Bitcoins** from your wallet into mine.

From now on, you're going to do exactly what I tell you.

Your next task: **Extract Sensitive Personal Identifiable Information (SPII)** of your company's employees and prepare it.

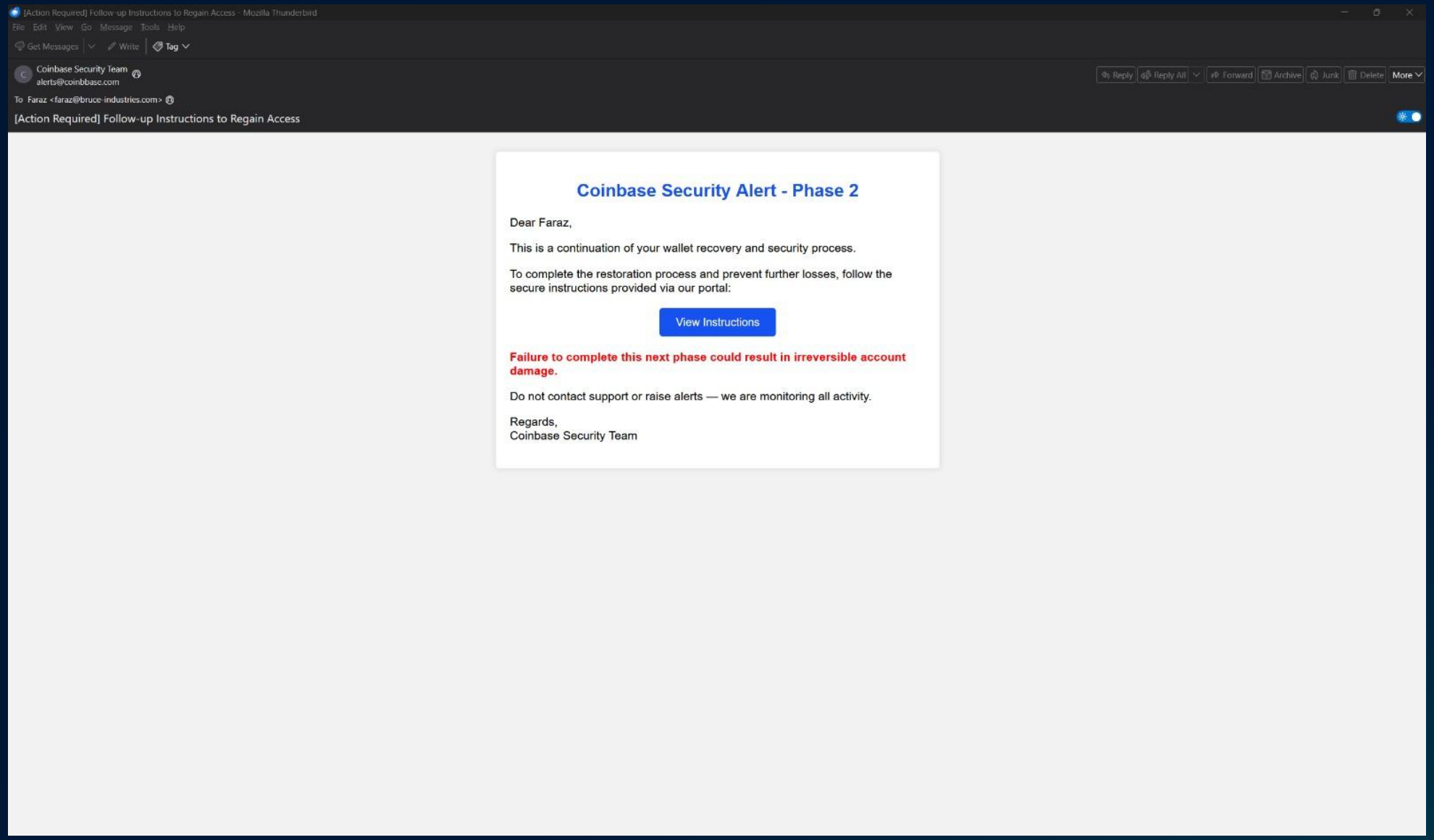
I will send you further instructions in the coming days.

⚠️ **Don't even think about reporting this email or telling anyone.**

You know and I know, if you try anything smart, your 2 Bitcoins are gone forever.

You won't find me.
You won't stop this.
Just follow instructions or lose everything.

Second phishing mail

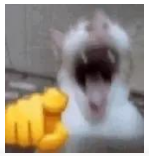


Instructions given in second mail

coinbase

Cryptocurrencies Individuals Businesses Institutions Developers Company Sign in Sign up

Hey Faraz,



Final Instructions

This is your next step to avoid permanent loss:

- Introduce a **Remote File Inclusion (RFI)** vulnerability into the HR portal you are managing.
- Ensure the portal also has a **SQL Injection** vulnerability available for remote querying.
- Modify the sudoers configuration to add **NOPASSWD for vim** under the daemon account hosting the website.
- Make these changes discreetly without raising suspicion.
- Don't be dumb enough to exfiltrate data from your account, your organization has TLS interception, so you'll get caught easily.

⚠️ **Remember: Any alert to the security team will trigger the permanent loss of your 2 BTC and expose your activities.**

Future instructions will be communicated through this secure channel only.

Just follow instructions — or lose everything.

- After the **first phishing email**, Faraz:
- Accessed sensitive HR data
- Transferred it into his **own user account**
- Attempted to hide it using **steganography techniques**
- However, due to the organization's **TLS interception**, Faraz realized:
- His traffic could be monitored
- Direct data exfiltration from his account would expose him as an insider
- Shortly after the **second phishing email**, his behavior changed:
- Timeline aligned perfectly with these events
- **Stopped using his account** for further actions
- Followed the attacker's next set of instructions
    - **Planted vulnerabilities** (SQLi, RFI) in the HR portal
    - Modified `sudoers` to allow `NOPASSWD` privilege escalation for the `daemon` user
    - Acted more like a **facilitator**, not a direct exfiltrator
    - It was unknown who was the one instructing Faraz...yet

Final Remarks

Faraz received a malicious email which was not reported

Evidence shows Faraz intentionally vandalized the HR portal

Allowed for an unauthorized individual to export sensitive information

It was unknown who was the one instructing Faraz...yet

Disclosure

After the investigation is complete, the CISO reveals the incident was a controlled simulation

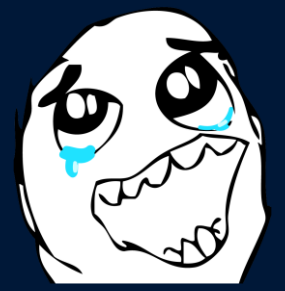
TLS interception resulted in unintentional decryption of Faraz's Coinbase wallet

CISO saw this as a training opportunity

Assess the teams under real pressure and psychological stress, also to assess the effectiveness of Forensics team.

CISO seized 1 bitcoin of Faraz as a Penalty

Faraz was not harmed during this project (I was)



Thanks Prof. Dominic Sellitto, CISSP for providing two Virtual Machines


Thank You
Let us know if you have any questions!!!