

PRISON BREAK

Team Cyberons

Ricardo Aranaga

Matthew Alvidrez

Sai Chaitanya Pothuraju

Chitti Lakshmi Deepak Doddigarla

What we used

- Jailing environments (SSH & FTP)
- Random ASCII Encryption
- 'cd ..' .bashrc Restriction
- Forwards and Backwards Stegging
- Covert Filepermission
- Timing covert channel



Layer 0

- Encrypted message is given to the participant and this encrypted message is generated by a new pattern.

< Message->Binary->Replace 1 or 0 with random odd or even ASCII value >

- Output: TCP Server credential information.**

List
a,b,c,d...A,B,C,...1,2,3,...0

B A Z I N G A

B						
1	0	0	0	0	1	0
a	b	b	d	z	a	2

A						
1	0	0	0	0	0	1
e	2	4	2	6	8	a

Z						
1	0	1	1	0	1	0
y	X	Y	3	4	9	2


I						
1	0	0	1	0	0	1
A	B	B	A	B	b	1

N						
1	0	0	1	1	1	0
C	D	D	E	E	Y	z

G						
1	0	0	0	0	1	1
1	0	0	0	1	1	1

A						
1	0	0	0	0	0	1
E	Z	0	0	0	0	A

Layer 1

- Client connects to a server and the server asks some questions to the client. If client answers them correctly, then server transmits messages with a time delay (Timing covert channel). The time delays are the multiples of 0.02 (i.e., 0.1, 0.2, 0.3 ... 1.0). The odd values(0.3 & 0.1) represent binary '1' and even values(0.04 & 0.06) represent binary "0".
 - The client will have 6 chances to answer the questions correctly with a time limit of 60s per question and their IP will be blocked after 6 wrong answers
 - **Output: SSH & FTP server credential information.**
- 

Layer 2a

- Client connects to the SSH server in a jailed environment with limited bash commands . A maze of folders with fake ones implanted that have to be traversed to find the correct folder, where a file is hidden. This Layer is meant to wear out the student until he remembers that in the previous layer (Timing covert) message, there is a hint that reveals two things:
 - This server can receive SSH and FTP connections (At the end of the message)
*HINT: PATIENCE IS A VIRTUE..... **FTP or SSH***
 - The username and password are inverted for the FTP server log in, and follow a pattern (CaPiTaLiZaTiOn).
*HINT: user: "billythekid", pass: "PatGarertt" **or the other way around***
- **Realization: ftp to server, credentials: user: "patgarret", pass: "BillyTheKid"**

Layer 2b

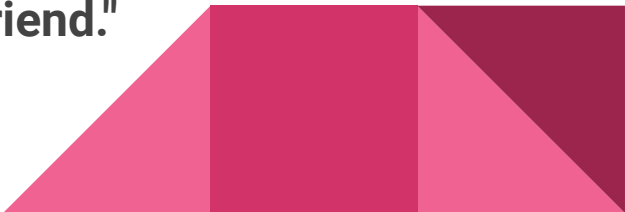
- Client connects to the FTP server in a jailed environment. Create a multitude of files, where a message is hidden in the file permissions. So, the client would have to use a program that deciphers a covert message in the file permissions of a list of files (7-bit/10-bit).

char -	P	R	I	S	O	N
ASCII -	80	82	73	83	79	78
	↓	↓	↓	↓	↓	↓
binary -	0001010000	0001010010	0001001001	0001010011	0001001111	0001001110
	↓	↓	↓	↓	↓	↓
fp -	__x_w__	__x_w_w__	__x_x_x__	__x_w_wx__	__x_xrwx__	__x_xrw__

- Output: Path location to an audio file

Layer 3

- Get the hidden file from the SSH server in the obtained path using the 'scp' command ("Superman/MichaelJackson/JantarMantar/MonkeyMia/")
- The audio file is stegged in the normal and reverse order. If the client finds the audio file before getting the instructions on how to stegg it (reversed). It will have a stegged image in an uncommon interval and offset that will provide a hint that they might be working on the wrong file.
- Output: **"We are captives of our own identities, living in prisons of our own creation.You've escaped the prison. Good luck my friend."**



Layers	Sub Tasks	Challenges	Ownership
0	ASCII Encryption & Decryption		Deepak
1	Timing covert channel		Matthew
	Multithreaded Server	Thread Termination Handling exceptions	
2 & 3	Jailing Environment	Libraries needed for smooth traversing	Ricardo
	Setting up the FTP & SSH	Switching home folders and permissions	Ricardo
	Restricting “cd” function	New to bash environment	Sai Chaitanya
	File Permissions covert channel		Sai Chaitanya
4	Multitude Folder creation & Reverse Stegging	Time consuming task	Deepak

Our scoring of the puzzle

For completing the layers

Layer 0 - 5000 Pts

Layer 1 - 10000 Pts

Layer 2 - 10000 Pts

Layer 3 - 25000 Pts

Total - 50000 Pts

Bonus Points

Cracking trivia in less than 3 attempts - 500Pts

Locating the audio without Puzzle 2 - 1500Pts

Extracting “ItsATrap” audio file from wrong file -1000Pts

Extracting GIF file by normal stegging - 1000 Pts



Bill Of Materials

For our challenge all of the material that we used are available in the CSC442/CYEN301 - Introduction to Cyber Security class. To be able to complete the challenge they should have everything available to them as long as they participated in the class.





DEMO