Note: Any classification markings are for training use only.

LIMITED RELEASE FOR

i5 Space Cyber Warfare Division

TOP SECRET//SCI

CHARLIE

CONTAINS SENSITIVE COMPARTMENTED INFORMATION

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATION SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDERS, STATUSES AND AGENCY IMPLEMENTING REGULATIONS.

TOP SECRET//SCI

CHARLIE

Operation Sky Tiger

FOR AUTHORIZED PERSONNEL ONLY

Note: Any classification markings are for training use only.

Sat0 – Brute Force Cracking – Intel:

i5 Special Forces have gained access to an encrypted file. They've uploaded it to a secure server here: https://bit.ly/41cVPEp

To crack the encrypted file we can attempt to guess the password. However, randomly making guesses ourselves would take way to long to crack. Using a tool called John the Ripper (or John), we can guess tens of thousands of passwords per second.

For the following commands, open a command line terminal using CTRL + ALT + T. Then type your commands and press enter to execute them.

Before we get started, here are some helpful commands:
List files:
$ ls
Change folder:
$ cd [folder_name]
Go back a folder:
$ cd ..
Go to your desktop:
$ cd ~/Desktop

Now, let's begin hacking.

To convert your encrypted zip file into a format John, our password cracker, can understand, use the command:

$ zip2john secret.zip > secret.hash

This command in plain English: *"Take secret.zip and create secret.hash using it in a format that John can understand."*

Now that John can read it, use John to find the password:

$ john secret.hash

When John finds a password it will stop running and print the password to the terminal.

We can unzip the file and use the password we found with John by using:

$ unzip secret.zip

The file “id_rsa” is an SSH key file. It gives whoever uses it special access to a system via a protocol called Secure Shell (SSH).

The satellite can be reached via SSH using the following login:

$ ssh admin@*IP* -p 5022 -i id_rsa

This command in plain English: *“give me a secure login as user admin to the server located at IP. Use port 5022 and my secret key found in the file id_rsa.”*

You can now disable the satellite by the command:

$ killsat

Sat1 – Decoding – Intel:

The Symposium Satellite Cluster (SSC) is made up of 3 satellites that orbit the earth and an associated 7 ground stations. They're all connected via a private network and accessible over IP.

i5 Special Forces have recently taken control of one of these ground stations. They've created a VPN tunnel into the network.

i5 Intel has discovered that Sat1 is running an SSH server located on port 5023 at the following IP address: _____. They've also obtained the SSH key file (sat1_key.zip located at https://bit.ly/41cVPEp for download, use password i5space to unzip). However, the SSH key file is encrypted so it cannot be used without the password.

During the raid i5 Special Forces also found the following hexadecimal code was present on a notepad with the title *"XOR SSH key"*:

84 89 95 8D 84 91 84 8B 82 8A

Using this information, the Intel team believes that the code may have something to do with unlocking the SSH key file.

Other red team assets operating parallel to yours have obtained a copy of the executable the server is based off of, and Intel believes that there is a hexadecimal XOR key located somewhere in the executable. The executable is located in the sat1_tools.zip file at https://bit.ly/41cVPEp for download. Your objective is to locate the key, decrypt the code, and shut down the enemy satellite.

To connect to SSH using the id_rsa key file, use:
$ ssh admin@[IP] -p [PORT] -i id_rsa

Sat2 – Reverse Engineering – Intel:

Background:

The Symposium Satellite Cluster (SSC) is made up of 3 satellites that orbit the earth and an associated 7 ground stations. They're all connected via a private network and accessible over IP.

i5 Special Forces have recently taken control of one of these ground stations. They've created a VPN tunnel into the network.

One of the foreign satellites in the SSC is running a vulnerable FTP server.

The satellite can be reached over IP: _____

Tiger Client Intel:

Intel has gained access to a CLI client for the system. The script, along with the client/server's shared library, can be found here: https://bit.ly/41cVPEp

Download and run the python scripts to load the CLI.

Command types and their parameters:

1. connect <username> <password>
2. get <file>
3. put <file>
4. exit

Intel has gained access to one of the system administrators login credentials. To connect to the server, use the following command:

> connect [ip] [username] [password]

Username: admin4
Password: harambe

Tiger Server Intel:

The server is a python script named **tigers.py**. The FTP client does not perform error checking on user input, so all files in the server's directory can be downloaded.

The server is running outdated version of the Tiger FTP system that still has commands implemented that the CLI no longer supports.