LIMITED RELEASE FOR
DETACHMENT 538

SECRET//SCI

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.

SECRET//SCI

FOR AUTHORIZED PERSONNEL ONLY
Note: Any classification markings are for training use only.

Operation Yellow Jacket

The country of Genorak has had extremist leaders who have been in power longer than a typical term for their government officials. A few months ago, Genorak invaded into Desomel, an allied country of the United States putting us at war with Genorak. Intelligence has shown that the Genorak military forces are being positioned to invade more countries. Your team has been tasked with crippling the infrastructure of the Genorak military by destroying a munitions plant located deep in Genorak territory. The munition plant is being protected by anit-aircraft munitions as well as the Genorak Defense Force. By crippling Gernorak's infrastructure, it will allow another US team to strike the leaders, freeing the people of Genorak.

The following documents contain specific information regarding your duties for this operation. Information within this document can not be shared with outside sources or anyone without authorization to view the sensitive documents.

LIMITED RELEASE FOR
DETACHMENT 538

0PERATI0N YELL0W JACKET

01010111 01100101 01101100 01100011 01101111 01101101 01100101

FOR AUTHORIZED PERSONNEL ONLY
Note: Any classification markings are for training use only.

Background

You are about to embark on a crucial mission. As a member of the 131st Cyber division of the Air Force, you will be working alongside the intel, ground, and air team to take down an enemy munitions plant.

The enemy air defenses are preventing our air team from bombing the munitions plant. The ground team will be able to shut down the power powering the air defenses. Your mission is to exploit vulnerabilities in the enemy satellite network, disabling all the satellites and then shut down the power to the SAMs. If we fail to take down the satellite network first, the enemy will be able to remotely restart the power, rendering our air team unable to take down the munitions plant. Your task is critical to the mission's success, and failure is not an option.

You will be working as part of a team of elite soldiers, each with unique skills and expertise. Together, you must exploit the satellite network's vulnerabilities, disable all the satellites, and cut off the power to the enemy air defenses.

The United States Intelligence has monitored these satellites for an extended period of time and gathered data on them. Listed below are the possible exploits the satellites may be vulnerable to. Good luck.

Vulnerabilities Information

SQL Injection -> Backdoor

AstroSec Defense is a prominent defense contractor specializing in advanced satellite technology. They were the primary contractor working on the Terrasat Network. Intel suggests that they built a backdoor shutdown code into several of their more recent satellites. These codes are reported to be on their servers and can remotely disable their satellites in case of emergencies.

Insecure Cryptosystems

Intel suggests that version 2.3.^ satellites are running a vulnerable implementation of the AES128 encryption scheme for data transfer.

Packet Sniffing

Intel reports that one of the v1.^ software patches fixed a vulnerability which transfers unencrypted password data with the Terrasat Operator Command and Control Application (TOCCA). Using Wireshark to snoop the packet data should reveal this vulnerability.

Payload Injection

Intel reports that some of the satellites were misconfigured and launched with debug mode still enabled. This debug mode gives scriptable root access to the satellite's operating system and control hardware.

Brute Force Cracking

Intel reports that some of the satellites have very short passwords protecting their admin logins. Utilizing a tool like John the Ripper would allow for rapid password checking.

Beamforming Plan Disruption

Intel reports that the satellites are equipped with an advanced beamforming system. Utilizing custom beamforming plans may allow destructive interference to disrupt the satellite fleet.

Buffer Overflow

Intel reports that the software used for interfacing with certain satellites within the network is outdated and makes use of now insecure functions. One function researchers have highlighted as being used frequently is the sprintf function in the C language, exposing these satellites to a buffer overflow attack.

Reverse Engineering

Intel has gained access to v2.4.^ satellite's comms module. They're unsure if any vulnerabilities exist. They would like you to reverse engineer it.