1 iCTF

1.1 iCTF 2015

Der iCTF (international Capture The Flag) wird jährlich von der University of California, Santa Barbara veranstaltet und ist der größten Hackerwettbewerbe dieser Art. Der iCTF integriert Angriff und Verteidigung zugleich. Die Teilnehmer müssen gleichzeitig Flaggen von fremden Servicen klauen, sowie ihre eigenen Service patchen um diese unangreifbar zu machen. Dieses Jahr fand der Wettbewerb am 04.12. statt und 36 Teams nahmen daran Teil. Dabei belegte unser Team (in23canation) den 22. Platz.

1.2 Aufbau und Configuration

1.3 Services: Dungeon

Der Dungeon Service war ein Consolenservice der ein Spiel darstellt. der Spieler muss dabei durch ein Dungeon laufen und am Ende einen Drachen töten. Um dies zu bewerkstelligen werden 2 Gegenstände gebraucht. Ein goldener Säbel und ein magisches Schild. Um den Säbel zu bekommen muss zuerst ein geheimer Raum gefunden werden in dem der Namen eines Flugzeuges anhand eines Abbilds erraten werden muss. Wird richtig geraten erhält der Spieler den Säbel. Des weiteren gibt es einen Raum, bei dem ein Zwerg sein Schild abgibt, wenn du seine Nummer errätst. Dies ist jedoch fast unmöglich da die Nummer zufällig bestimmt wird. Des weiteren bekommt man den Schild ebenfalls nicht wenn man die Nummer errät. Um diesen nun zu bekommen muss in einem anderen Raum bei einem Gnom der nach den Spielernamen fragt den Speicher überschreiben. Die Funktion übergibt die Adresse der Variable HAVE_SHIELD und wenn man ein beliebiges Zeichen und dann %n eingibt, wird auf der Adresse HAVE_SCHIELD eine 1 eingetragen. Wenn der Spieler nun beim Drachen ist, stirbt er nicht wie sonst, sondern kann den Drachen mit dem command “kill dragon“ töten. Im Anschluss daran wird er Spieler erneut nach seinem Namen gefragt. Nun kann man mithilfe eines Bufferoverflows die Rücksprungadresse der Funktion so ändern, dass der Spieler im Secret Storage Room landet. Dort wird die Flagge ausgegeben, wenn die ID angegeben wird. Eine Hürde beim Bufferoverflow ist jedoch, dass auf eine Variable geprüft wird und wenn die überschrieben wird, wird der Nutzer vom Service getrennt. Um dies zu verhindern muss genau ab der 88. Stelle 0xDEADBEEF in ASCII mitübergeben werden. Danach noch 4 Zufallszeichen und dann die Rücksprungadressse. 0xDEADBEEF sowie die Rücksprungadresse müssen umgedreht werden, das litte Endian verwendet wird.