**Cylert CTF Challenge Writeup**

**Hello everyone, it was my pleasure to meet you all at the CDIS Conference last week.**

**I had the opportunity to make a simple network challenge and I was delighted to have good feedback about the challenge. The challenge is aimed for beginner to early intermediate CTF players. Let’s dive to the writeup right away.**

**The challenge was hosted on the local network on the IP 111.111.10.209 but I wrote this writeup on my local network so the IP will be different in screenshots.**

**We start with the basic Nmap scan using the -p- argument to scan All ports.**

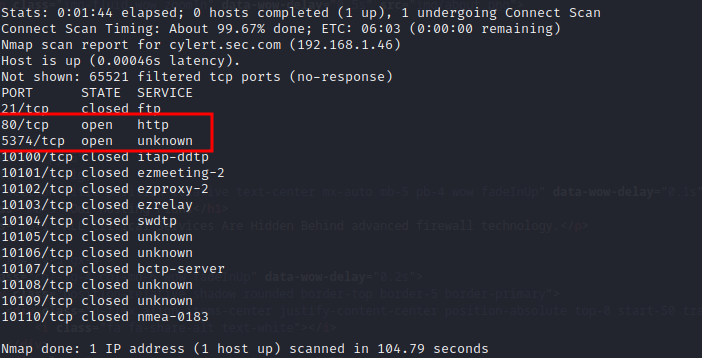
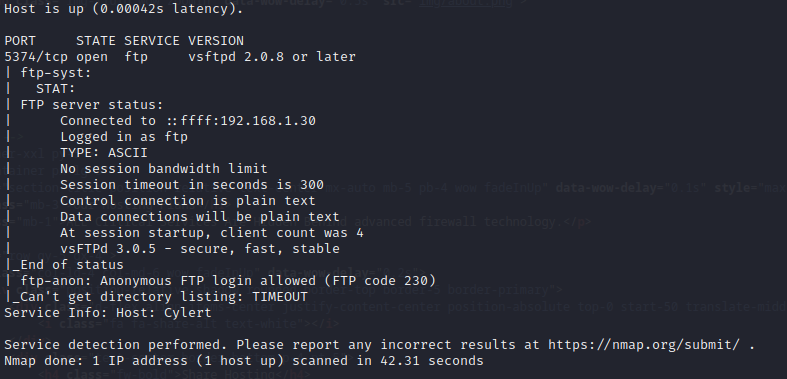
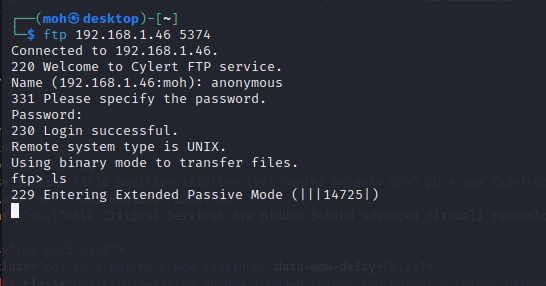


Figure 1 open ports

**We have 2 open ports 80 and 5374. Scanning the strange port with Nmap scripting engine we had the following results.**

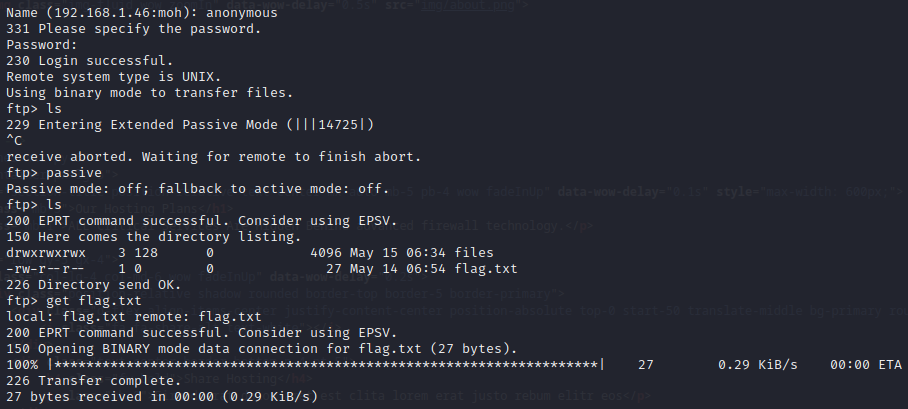


**It has ftp service running and anonymous login is allowed. Lets try logging in.**

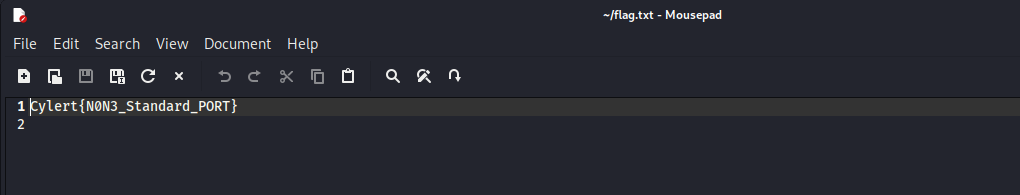


**We tried to execute simple commands but as you can see in the above screenshot it says it is entering passive mode then nothing happens.**

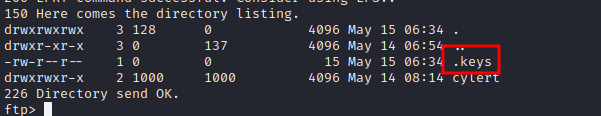
**So, we disabled passive mode as you can see below.**



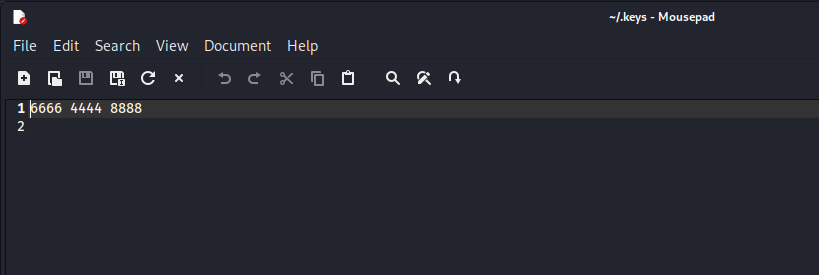
**Now commands are executed normally and we managed to list files on the box. We finally got our first flag.**



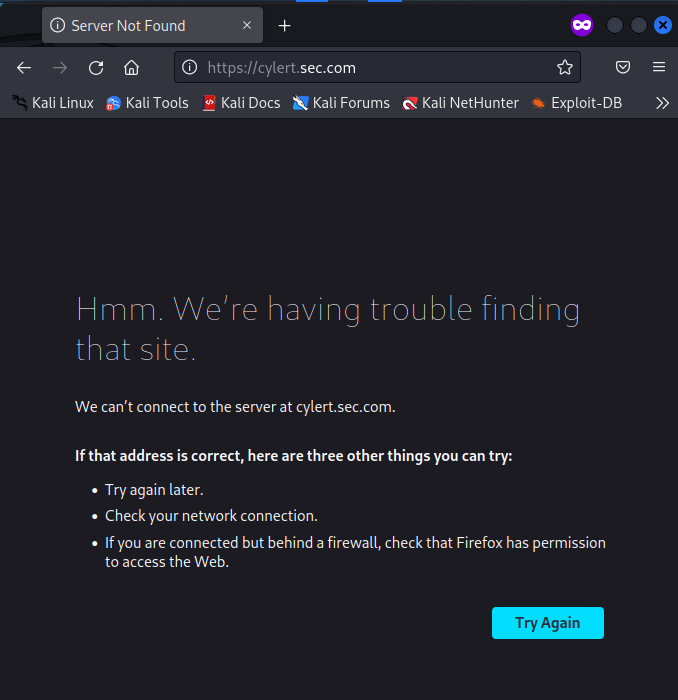
**Then we tried to list hidden files in the “files” directory and we got a file called keys.**



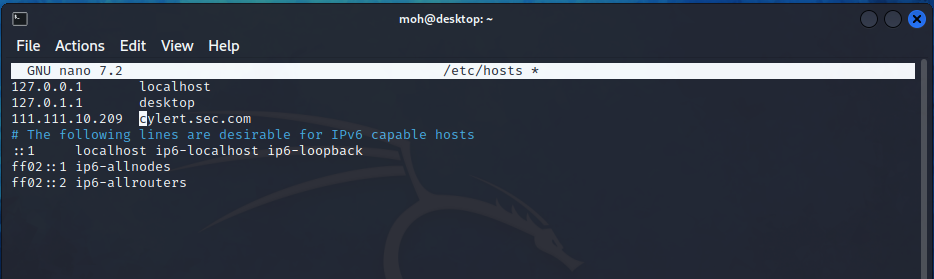
**This file contained what seemed like ports.**



**We will leave this for now and move to port 80. After visiting site we were faced with the below response.**



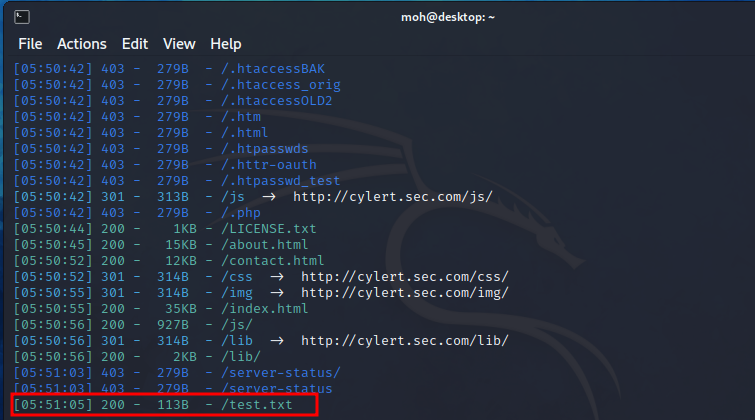
**Which means that we need to modify our /etc/hosts to point to this virtual host name.**



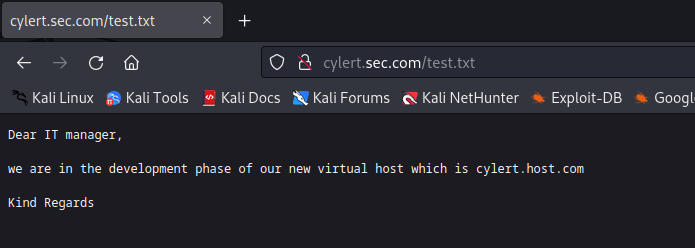
**After that we can navigate to this host where we find a company page called “Safe Cam”.**



**Directory busting on the web servers may be essentials to reveal hidden files or directories on the web server so we ran “dirsearch” tool and we found an interesting test.txt file.**



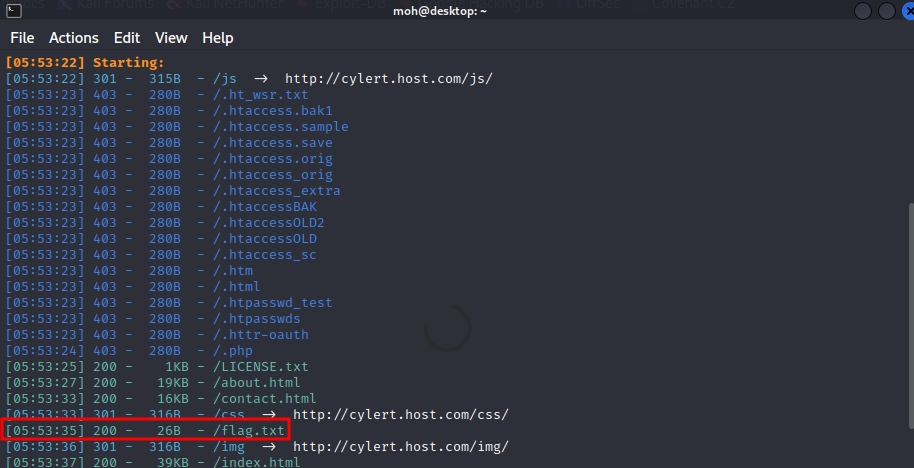
**Navigating to this file revealed another virtual host which is Cylert.host.com.**

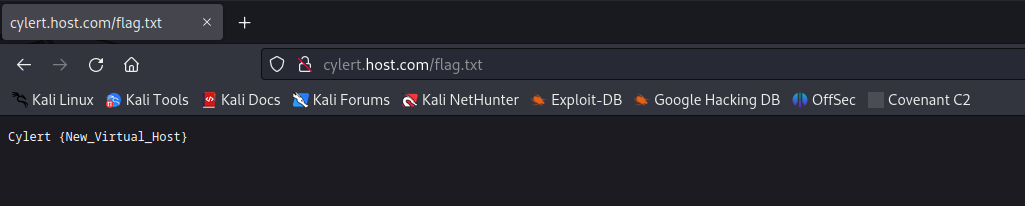


**Adding this host to the /etc/hosts made this host available to us.**

**Navigating to this virtual host reveals another website called greenhouse for hosting services.**

**Also using “dirsearch” tool on this virtual host reveal the second flag. As you can see below.**



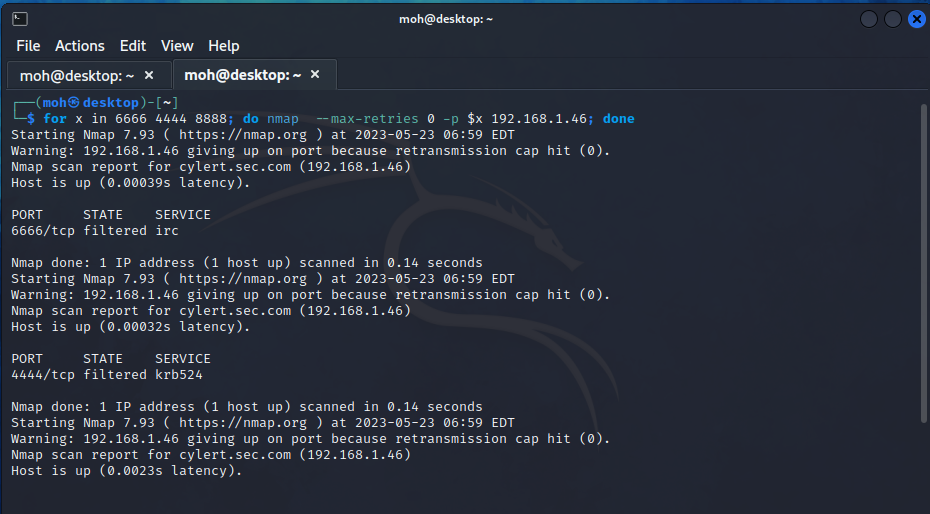


**The source code of this web site page reveals an interesting info.**

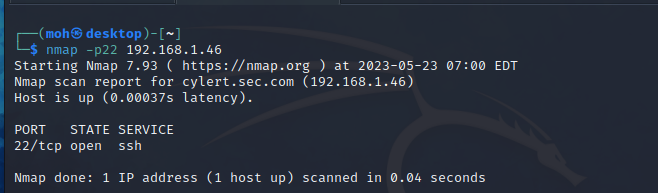


**With this info and the hidden “keys” file we were sure that this box has port knocking technique enabled. And the sequence of ports that we had earlier is the key to open the SSH service.**

**We used NMAP to do the knocking part as you can see below.**

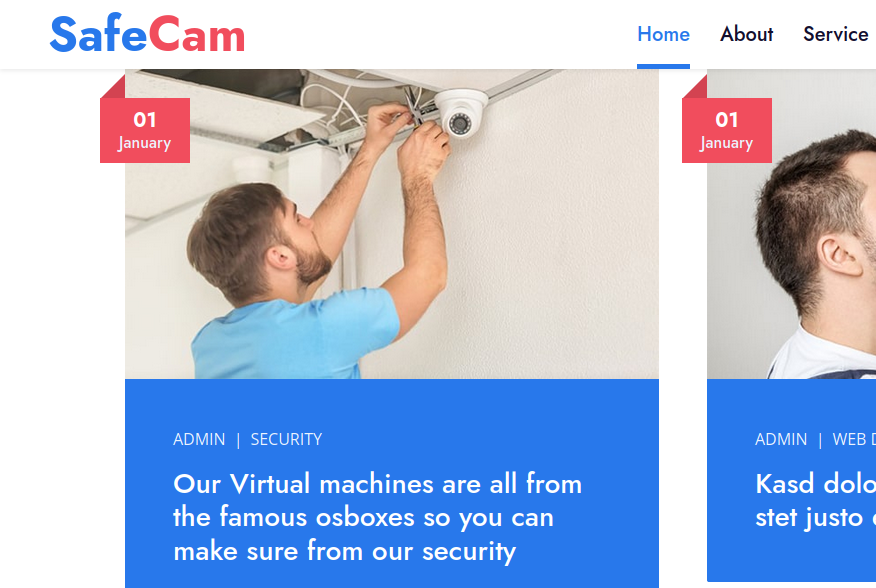


**When we do NMAP scan again we find that SSH port is now open.**



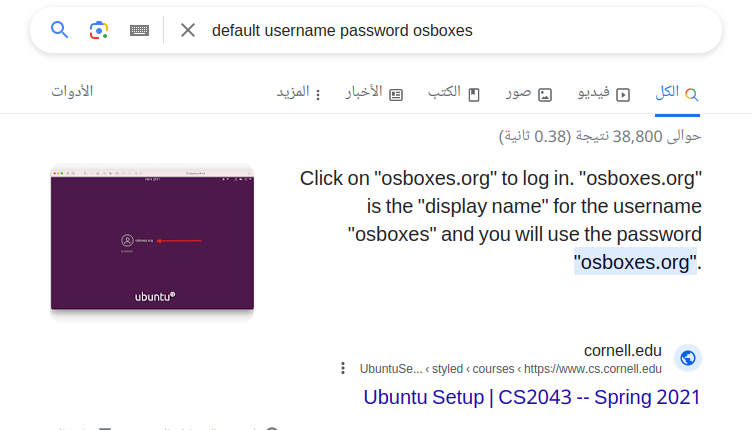
**But we don’t have credentials to access the SSH service. We must have missed something.**

**So Going through the Safe Cam website we find 2 pieces of info. The box uses virtual machines form OSBOXES website.**

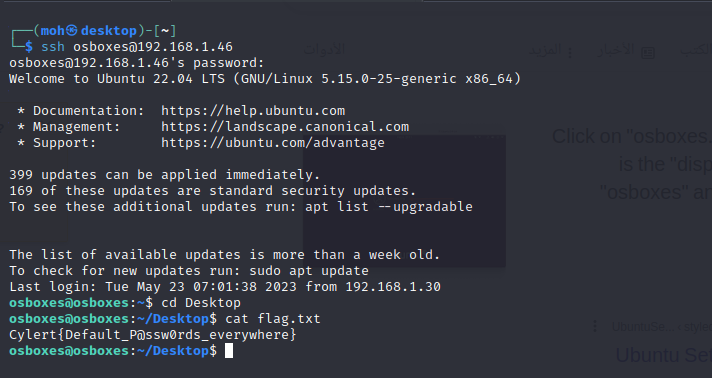


**This info was also mentioned at the footer of the web page.**



**Using this info, we head to google to search about OSBOXES and we found that the default credentials for the virtual machines is “osboxes.org” with the username OSBOXES.** 

**So eventually we try this combination of username and password on the newly found SSH service and we are in! And we got the last Flag.**



**And now we come to the end of this writeup. I really enjoyed making this challenge and I hope you all enjoyed solving it at the conference.**