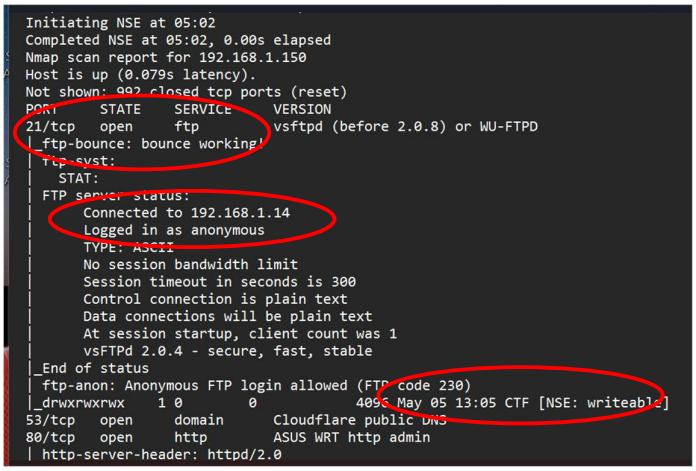
Once past the WEP encrypted router,

I started with a basic nmap scan and found a few open ports.

```
Completed Parallel DNS resolution of 1 host. at 04:
Initiating SYN Stealth Scan at 04:59
Scanning 192.168.1.150 [1000 ports]
Discovered open port 21/tcp on 192.168.1.150
Discovered open port 445/tcp on 192.168.1.150
Discovered open port 139/tcp on 192.168.1.150
Discovered open port 80/tcp on 192.168.1.150
Discovered open port 53/tcp on 192.168.1.150
Discovered open port 8200/tcp on 192.168.1.150
Discovered open port 515/tcp on 192.168.1.150
```

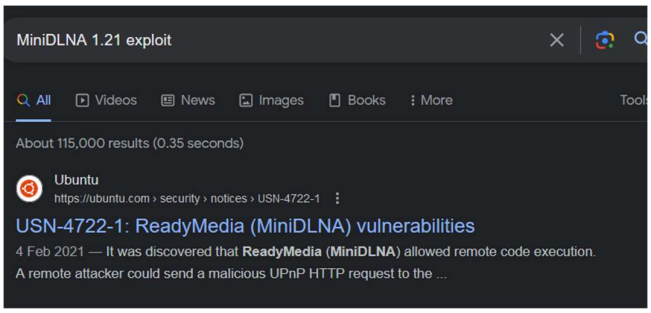
Next, I just threw every NSE script at it with Nmap -A and found 2 interesting banners.




```
80/tcp   open     http        ASUS WRT http admin
|_http-server-header: httpd/2.0
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     ▯▯▯r▯U      Samba smbd 3.0.33 (workgroup: WORKGROUP)
514/tcp  filtered shell
515/tcp  open     tcpwrapped
8200/tcp open     upnp        MiniDLNA 1.2.1 (Linux 2.6.36; DLNADOC 1.50; UPnP 1.0)
```

A **CTF folder was accessible** through ftp anonymous login on port 21.

Port 8200 had a vulnerable media player with possible RCE



Flag.txt was found 2 directories deep in the CTF Folder.