

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 04:58
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.

```
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Nmap scan report for 192.168.1.150
Host is up (0.079s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd (before 2.0.8) or WU-FTPd
ftp-bounce: bounce working!
ftp-svst:
STAT:
FTP server status:
  Connected to 192.168.1.14
  Logged in as anonymous
  TYPE: ASCII
  No session bandwidth limit
  Session timeout in seconds is 300
  Control connection is plain text
  Data connections will be plain text
  At session startup, client count was 1
  vsFTPD 2.0.4 - secure, fast, stable
End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
dnwrxrwxrwx 1 0 0 4096 May 05 13:05 CTF [NSE: writeable]
53/tcp    open  domain  Cloudflare public DNS
80/tcp    open  http     ASUS WRT http admin
http-server-header: httpd/2.0
```

```
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  smb        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.

