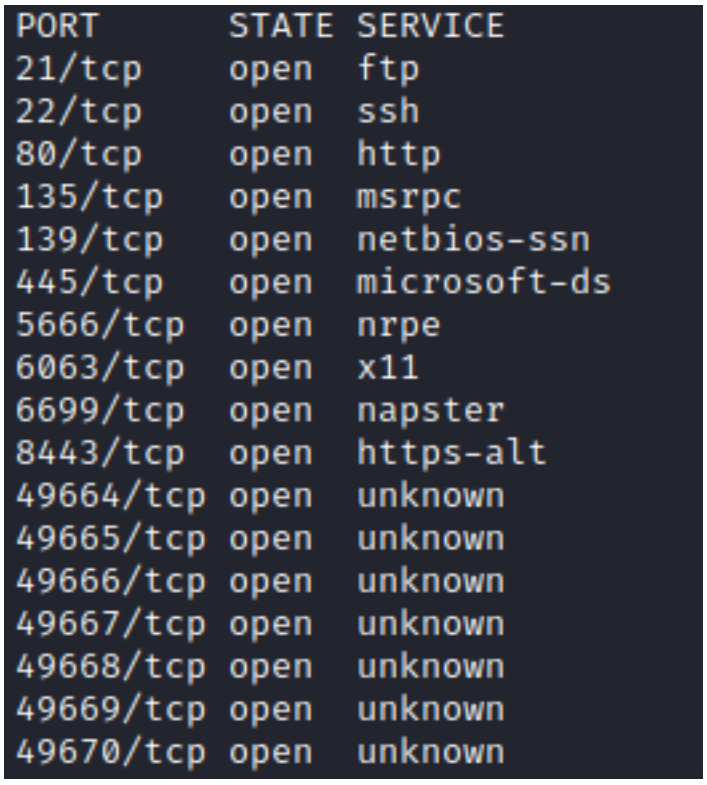
Servmon

TOP 1000:

```
└─$ nmap -sC -sV -Pn -oN nmap/init.nmap 10.10.10.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-29 21:32 EDT
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 21:35 (0:00:14 remaining)
Nmap scan report for 10.10.10.184
Host is up (0.087s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE    SERVICE       VERSION
21/tcp   open     ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-28-22  07:35PM       <DIR>          Users
| ftp-syst:
|_  SYST: Windows_NT
22/tcp   open     ssh           OpenSSH for_Windows_8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
|_  256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
135/tcp  open     msrpc         Microsoft Windows RPC
445/tcp  open     microsoft-ds?
464/tcp  filtered kpasswd5
3826/tcp filtered wormux
5666/tcp open     tcpwrapped
6699/tcp open     napster?
8443/tcp open     ssl/https-alt
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after:  2021-01-13T13:24:20
| http-title: NSClient++
|_Requested resource was /index.html
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 404
|     Content-Length: 18
|     Document not found
|   GetRequest:
|     HTTP/1.1 302
|     Content-Length: 0
|     Location: /index.html
|     iday
|_    :Saturday
1 service unrecognized despite returning data. If you know the service/version,
SF-Port8443-TCP:V=7.94%T=SSL%I=7%D=8/29%Time=64EE9CA0%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,74,"HTTP/1\.1\x20302\r\nContent-Length:\x200\r\nLocation
```

ALL PORTS:



Somehow top 1000 scan missed port 80... but it is open :D

enumeration

ftp anonymous login allowed. we find two files

talks about a password at passwords.txt at Nathan's desktop

we discover that the website has an LFI. (idk why but only works with burpsuite)

Gives a password list:

1nsp3ctTh3Way2Mars!

Th3r34r3To0M4nyTrait0r5!

B3WithM30r4ga1n5tMe

L1k3B1gBut7s@W0rk

0nly7h3y0unGWi11F0l10w

IfH3s4b0Utg0t0H1sH0me

Gr4etN3w5w17hMySk1Pa5$

ssh

We will perform a password spray attack with the password list we gathered, and the two possible usernames found from ftp (Nathan and Nadine)

We can do this with metasploit's scanner/ssh/ssh_login
It worked!

Nadine:L1k3B1gBut7s@W0rk

priv esc

Enumerating the file system, we find NSClient++

Then,
Get-Content .\nsclient.ini reveals config information, including a password: ew2x6SsGTxjRwXOT

Also,
PS C:\Program Files\NSClient++> .\nscp.exe --version
NSClient++, Version: 0.5.2.35 2018-01-28, Platform: x64
-> https://www.exploit-db.com/exploits/46802