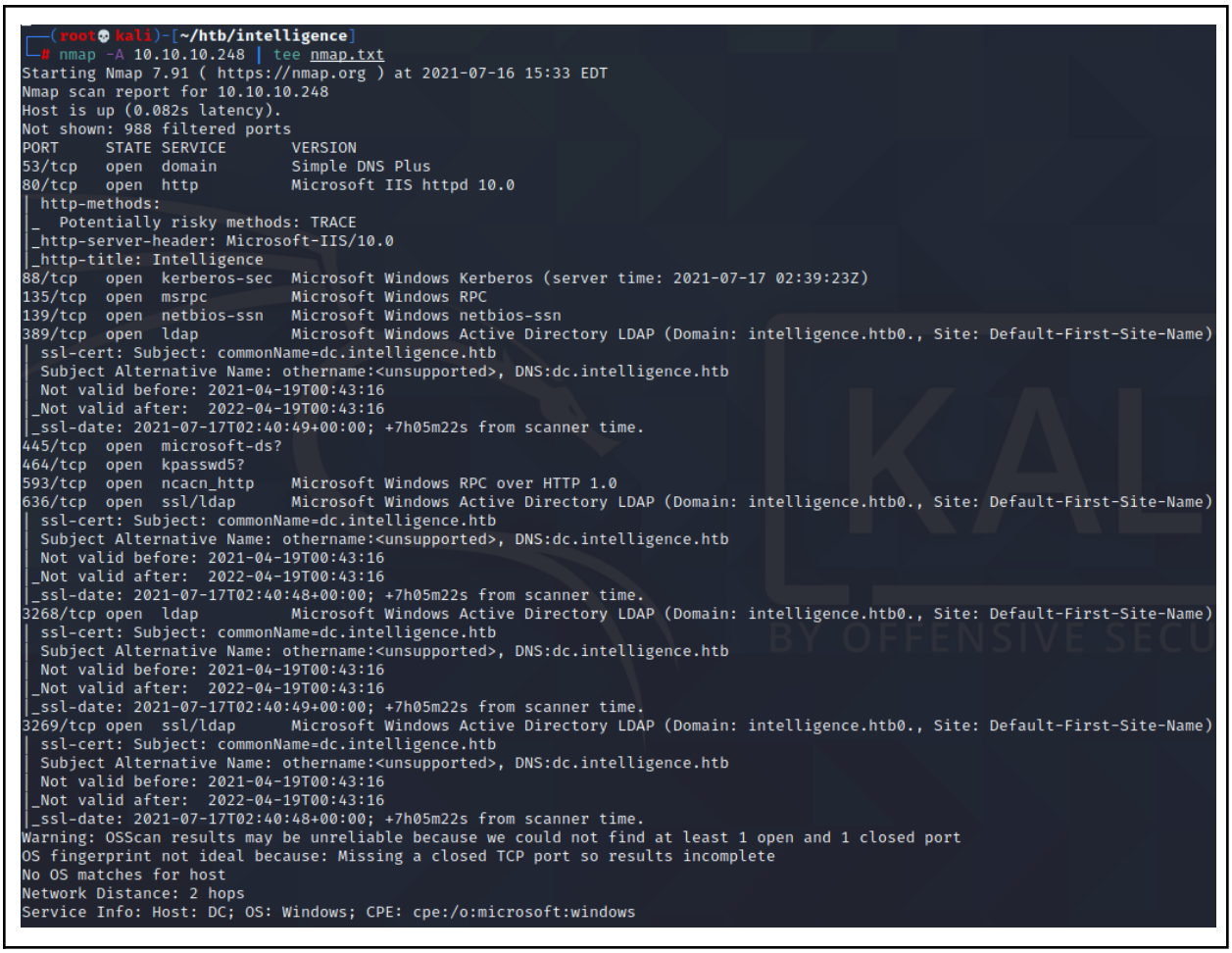
Intelligence

Difficulty: Medium
OS: Windows

Nmap

Starting off with our aggressive nmap scan, we see ports 53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 3268, and 3269 are open. A lot of these have to do with ldap so we assume that is the place to search, but first a little enumeration.



```
┌──(root💀kali)-[~/htb/intelligence]
└─# nmap -A 10.10.10.248 | tee nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-16 15:33 EDT
Nmap scan report for 10.10.10.248
Host is up (0.082s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Intelligence
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-07-17 02:39:23Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
|_ssl-date: 2021-07-17T02:40:49+00:00; +7h05m22s from scanner time.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
|_ssl-date: 2021-07-17T02:40:48+00:00; +7h05m22s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
|_ssl-date: 2021-07-17T02:40:49+00:00; +7h05m22s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Not valid before: 2021-04-19T00:43:16
|_Not valid after:  2022-04-19T00:43:16
|_ssl-date: 2021-07-17T02:40:48+00:00; +7h05m22s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Enumeration

Looking around smb and rpc, we find nothing of use.

Performing a fuzz scan brings back only one web directory, “documents”. Attempting to go to this directory on the web server results in a 403 error.

Going over to ldap, we begin by gathering some basic information about the service. First, we pull out python3 to execute some commands to connect to ldap. Attempts to use ldapsearch show connection errors, so we use custom python commands.

```
┌──(root💀kali)-[~/htb/intelligence]
└─# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server = ldap3.Server('10.10.10.248', get_info = ldap3.ALL, port = 636, use_ssl = True)
>>> connection = ldap3.Connection(server)
>>> connection.bind()
True
>>>
```

import ldap3
server = ldap3.Server('x.X.x.X', get_info = ldap3.ALL, port =636, use_ssl = True)
connection = ldap3.Connection(server)
connection.bind()

With our python commands, we have successfully made a connection to the ldap service. Now we can query for some basic information.

```
Naming contexts:
  DC=intelligence,DC=htb
  CN=Configuration,DC=intelligence,DC=htb
  CN=Schema,CN=Configuration,DC=intelligence,DC=htb
  DC=DomainDnsZones,DC=intelligence,DC=htb
  DC=ForestDnsZones,DC=intelligence,DC=htb
```

server.info

We could have also acquired this information through nmap’s “**ldap-rootdse.nse**” script

Going around ldap seems to do nothing. Stepping back, we go look at the website again and see there are some fairly useless documents there. However, these documents are named in a specific way. They begin with the year, month, and day, then end with "-upload.pdf". If we can construct our own wordlist and fuzz for pdfs, we may find something interesting.

First, we create a bash script to generate all the days in the year 2020. When we execute this, we redirect it to a file called "dates.txt". After we have this file, we concatenate "-upload.pdf" to every line to complete the wordlist.

```
#!/bin/bash
for i in {1..365};
        do
                date -I -d "2020-01-01 + $i days"
        done
```

```
┌──(root💀kali)-[~/htb/intelligence]
└─# sed -e 's/$/-upload.pdf/' -i dates.txt
```

```
2020-01-02-upload.pdf
2020-01-03-upload.pdf
2020-01-04-upload.pdf
2020-01-05-upload.pdf
2020-01-06-upload.pdf
2020-01-07-upload.pdf
```

Sed -e 's/$-upload.pdf/' -i dates.txt

Performing another fuzz scan, but this time in "/documents", we acquire a number of pdfs.

Before we go and painstakingly attempt to look at each of these files, we are also going to generate a list for 2021 and 2019. Doing so and running a fuzz scan also shows a few more documents

```
2021-01-14-upload.pdf   [Status: 200, Size: 10800, Words: 170, Lines: 137]
2021-01-30-upload.pdf   [Status: 200, Size: 24979, Words: 227, Lines: 194]
2021-01-03-upload.pdf   [Status: 200, Size: 26843, Words: 233, Lines: 206]
2021-02-10-upload.pdf   [Status: 200, Size: 26034, Words: 230, Lines: 205]
2021-03-01-upload.pdf   [Status: 200, Size: 10870, Words: 175, Lines: 135]
2021-01-25-upload.pdf   [Status: 200, Size: 26593, Words: 237, Lines: 215]
2021-03-07-upload.pdf   [Status: 200, Size: 10378, Words: 164, Lines: 139]
2021-02-13-upload.pdf   [Status: 200, Size: 26086, Words: 232, Lines: 212]
2021-02-21-upload.pdf   [Status: 200, Size: 25111, Words: 241, Lines: 214]
2021-03-27-upload.pdf   [Status: 200, Size: 11724, Words: 166, Lines: 141]
2021-02-25-upload.pdf   [Status: 200, Size: 25730, Words: 228, Lines: 180]
2021-03-10-upload.pdf   [Status: 200, Size: 24222, Words: 240, Lines: 199]
2021-03-18-upload.pdf   [Status: 200, Size: 27067, Words: 220, Lines: 203]
2021-03-21-upload.pdf   [Status: 200, Size: 25846, Words: 229, Lines: 205]
2021-03-25-upload.pdf   [Status: 200, Size: 26368, Words: 231, Lines: 211]
```