Return

nmap

```
# Nmap 7.94 scan initiated Sat Jul 22 00:55:45 2023 as: nmap -sC -sV -oN nmap/init.nmap 10.10.11.108
Nmap scan report for 10.10.11.108
Host is up (0.084s latency).
Not shown: 988 closed tcp ports (conn-refused)
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: HTB Printer Admin Panel
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-07-22 05:14:31Z)
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: return.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-07-22T05:14:41
|_  start_date: N/A
|_clock-skew: 18m33s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

interesting

We have access to the printer's admin panel on port 80
We can configure it to talk to us instead of the box, and it sends creds in plaintext

svc-printer:1edFg43012!!
→ login with winrm

as svc-printer, we are a Server Operator, which can configure services, and start/stop them
by setting the path of a service, we can execute anything as root

creating a meterpreter payload, we can upload using winrm and get a reverse shell as root