# Forest

## Nmap

```
sudo nmap -Pn -sV -p- 10.10.10.161 -oN nmap.txt
```

```
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNS-SD-TCP:OPTIONS
|   \x80\xAD
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-
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: htb.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393 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: htb.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open  mc-nmf        .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49684/tcp open  msrpc        Microsoft Windows RPC
49685/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you have a lot of time
SF-Port53-TCP:V=7.80%I=7%D=10/12%Time=5F8A0A7D%P=x86_64-pc-linux-gnu%r(DNS-
SF:SD-TCP:OPTIONS,2B,\x80\xAD\x81\x04\0\0\0\x01\0\0\0\0\0\0\x07_dns-sd\x04_
SF:tcp\x05local\0\0\x10\0\x01\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11n
SF:oldefault=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11dr=tcp\xC0\x0C
SF:\0\x10\x80\x01\0\0\x11\x94\0\x12\x11sm=tcp\xC0\x0C\0\x10\x80\x01\0\0\x1
SF:1\x94\0\x12\x11sv=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ms=tcp
SF:\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ver=tcp\xC0\x0C\0\x10\x80\x
SF:01\0\0\x11\x94\0\x12\x11ldap=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x1
SF:2\x11kpasswd=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos=tc
SF:p\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos-sec=tcp\xC0\x0C\0
SF:\x10\x80\x01\0\0\x11\x94\0\x12\x11winshadow=tcp\xC0\x0C\0\x10\x80\x01\0
SF:\0\x11\x94\0\x12\x11gc=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11p
SF:y=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11dns=tcp\xC0\x0C\0\x10\
SF:x80\x01\0\0\x11\x94\0\x12\x11dns-dynupdate=tcp\xC0\x0C\0\x10\x80\x01\0\
SF:0\x11\x94\0\x12\x11dns-tcp=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\
SF:x11dns-udp=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11mt=tcp\xC0\x0
SF:C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11pdc=tcp\xC0\x0C\0\x10\x80\x01\0\0\
SF:x11\x94\0\x12\x11gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\
SF:x11domain=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11dcr._msdcs=tcp
SF:\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11msdcs=tcp\xC0\x0C\0\x10\x80
SF:\x01\0\0\x11\x94\0\x12\x11ldap._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11
SF:\x94\0\x12\x11kerberos._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x
SF:12\x11kerberos-sec._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x
SF:11gc._msdcs._tcp=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11pdc._ms
SF:dcs._tcp=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11dr._msdcs._tcp
SF:=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11dc._msdcs._tcp=tcp\xC0\
SF:x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\
SF:0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\
SF:0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C\
SF:0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x
SF:10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x
SF:80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x
SF:01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x
SF:01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x
SF:01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x80\x01
SF:\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\
SF:0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x1
SF:1\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x1
SF:1\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x1
SF:1\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\
SF:x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94
SF:\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x
SF:12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x
SF:12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x
SF:12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12
SF:\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x1
SF:1ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ke
SF:rberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11k
SF:erberos._udp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11
SF:ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ld
SF:ap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap.
SF:_tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos
SF:._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerbero
SF:s._udp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._
SF:tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tc
SF:p.gc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.d
SF:c._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.
SF:dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp
SF:.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pd
SF:c._msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._
SF:msdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msd
SF:cs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._ms
SF:dcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._m
SF:sdcs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msd
SF:cs=tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=
SF:tcp\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp
SF:\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp
SF:\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp
SF:\xC0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\x
SF:C0\x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\
SF:x0C\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C
SF:\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C
SF:\0\x10\x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C
SF:\0\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0
SF:\x10\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x1
SF:0\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x
SF:80\x01\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\
SF:x80\x01\0\0\x11\x94\0\x12\x11kerberos._udp.dc._msdcs=tcp\xC0\x0C\0\x10
SF:\x80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.pdc._msdcs=tcp\xC0\x0C\0\x10\x
SF:80\x01\0\0\x11\x94\0\x12\x11ldap._tcp.gc._msdcs=tcp\xC0\x0C\0\x10\x80\
SF:x01\0\0\x11\x94\0\x12\x11ldap._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x01
SF:\0\0\x11\x94\0\x12\x11kerberos._tcp.dc._msdcs=tcp\xC0\x0C\0\x10\x80\x0
SF:1
```