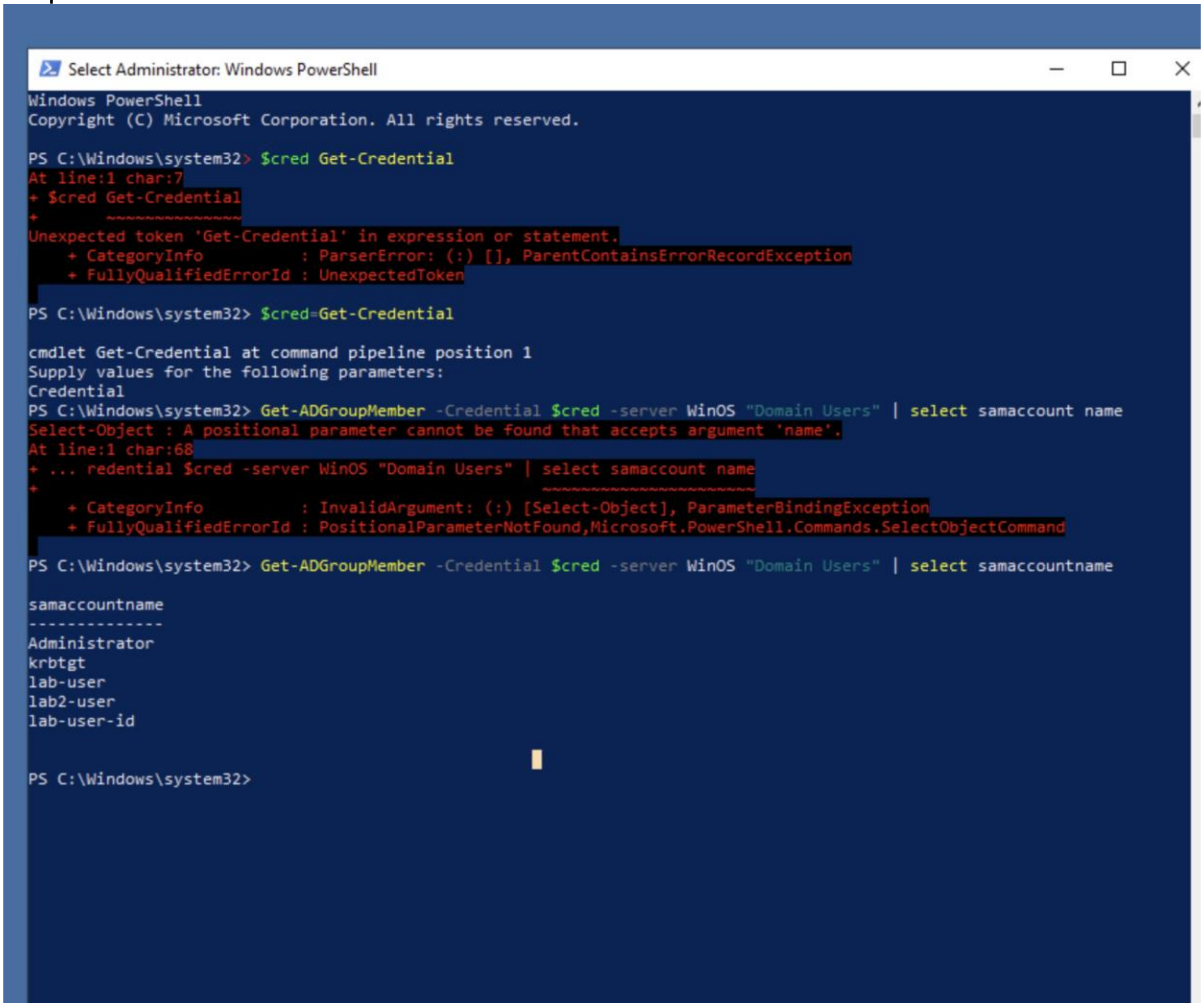
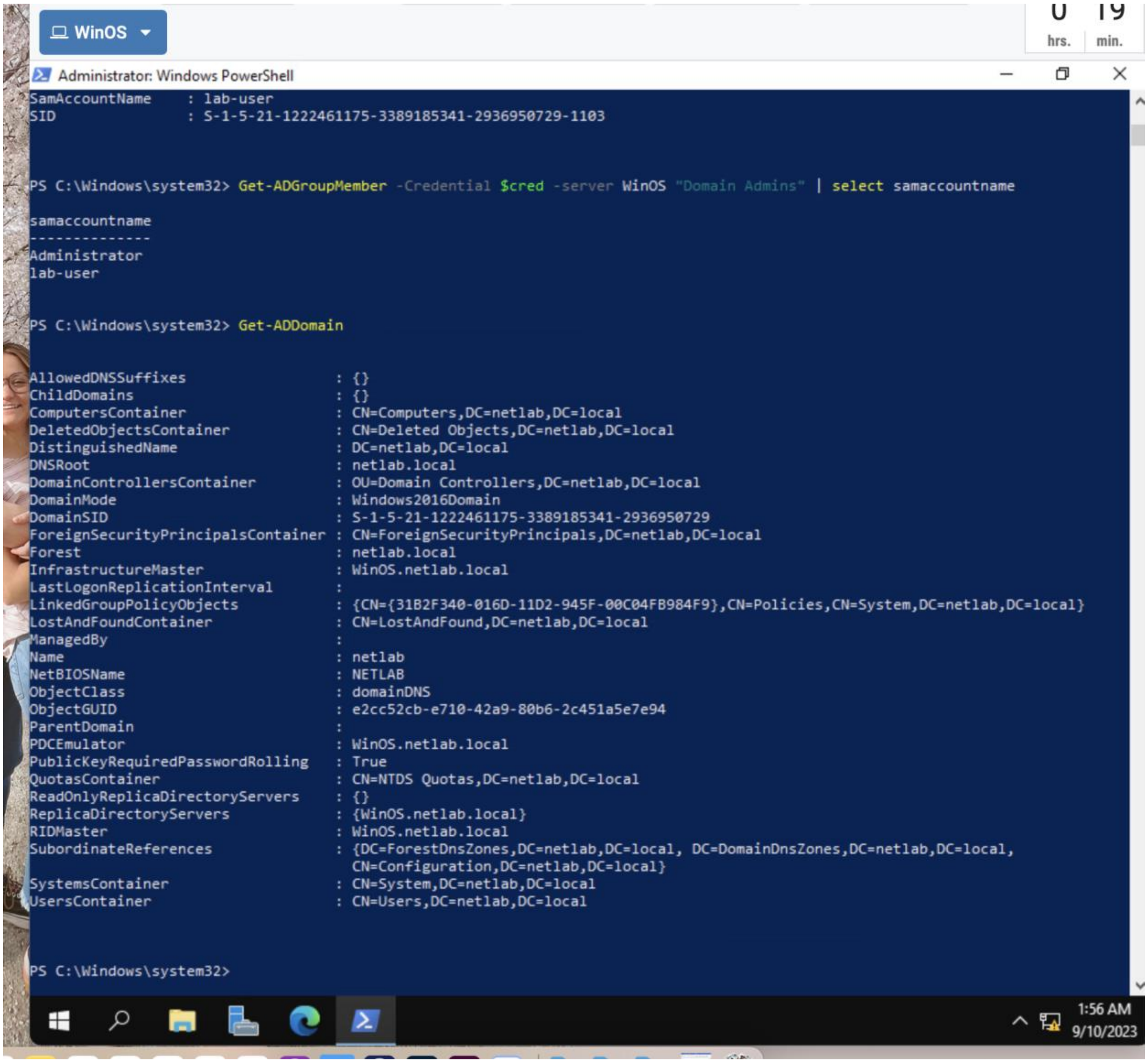
Peter Sanford
IT 2700
NetLab Lab 7
9/9/2023

1:
Step 7



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $cred Get-Credential
At line:1 char:7
+ $cred Get-Credential
+       ~~~~~~~~~~~~~~
Unexpected token 'Get-Credential' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Windows\system32> $cred=Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server WinOS "Domain Users" | select samaccount name
Select-Object : A positional parameter cannot be found that accepts argument 'name'.
At line:1 char:68
+ ... redential $cred -server WinOS "Domain Users" | select samaccount name
+                                                    ~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Select-Object], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SelectObjectCommand

PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server WinOS "Domain Users" | select samaccountname

samaccountname
--------------
Administrator
krbtgt
lab-user
lab2-user
lab-user-id


PS C:\Windows\system32>
```

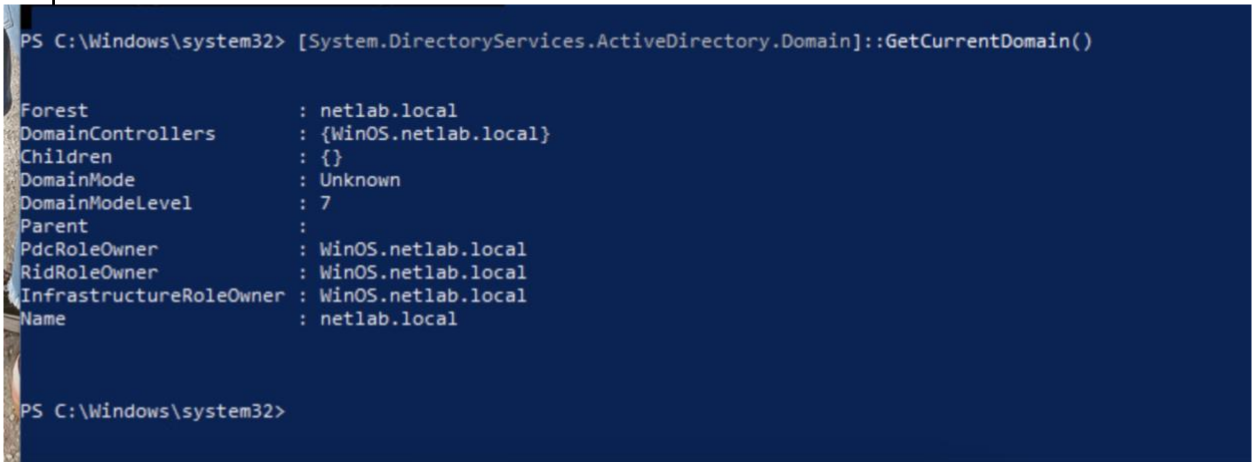
Step 10



```
SamAccountName    : lab-user
SID               : S-1-5-21-1222461175-3389185341-2936950729-1103


PS C:\Windows\system32> Get-ADGroupMember -Credential $cred -server WinOS "Domain Admins" | select samaccountname

samaccountname
--------------
Administrator
lab-user


PS C:\Windows\system32> Get-ADDomain


AllowedDNSSuffixes                 : {}
ChildDomains                       : {}
ComputersContainer                 : CN=Computers,DC=netlab,DC=local
DeletedObjectsContainer            : CN=Deleted Objects,DC=netlab,DC=local
DistinguishedName                  : DC=netlab,DC=local
DNSRoot                            : netlab.local
DomainControllersContainer         : OU=Domain Controllers,DC=netlab,DC=local
DomainMode                         : Windows2016Domain
DomainSID                          : S-1-5-21-1222461175-3389185341-2936950729
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=netlab,DC=local
Forest                             : netlab.local
InfrastructureMaster               : WinOS.netlab.local
LastLogonReplicationInterval       :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=netlab,DC=local}
LostAndFoundContainer              : CN=LostAndFound,DC=netlab,DC=local
ManagedBy                          :
Name                               : netlab
NetBIOSName                        : NETLAB
ObjectClass                        : domainDNS
ObjectGUID                         : e2cc52cb-e710-42a9-80b6-2c451a5e7e94
ParentDomain                       :
PDCEmulator                        : WinOS.netlab.local
PublicKeyRequiredPasswordRolling   : True
QuotasContainer                    : CN=NTDS Quotas,DC=netlab,DC=local
ReadOnlyReplicaDirectoryServers    : {}
ReplicaDirectoryServers            : {WinOS.netlab.local}
RIDMaster                          : WinOS.netlab.local
SubordinateReferences              : {DC=ForestDnsZones,DC=netlab,DC=local, DC=DomainDnsZones,DC=netlab,DC=local,
                                     CN=Configuration,DC=netlab,DC=local}
SystemsContainer                   : CN=System,DC=netlab,DC=local
UsersContainer                     : CN=Users,DC=netlab,DC=local


PS C:\Windows\system32>
```

2:

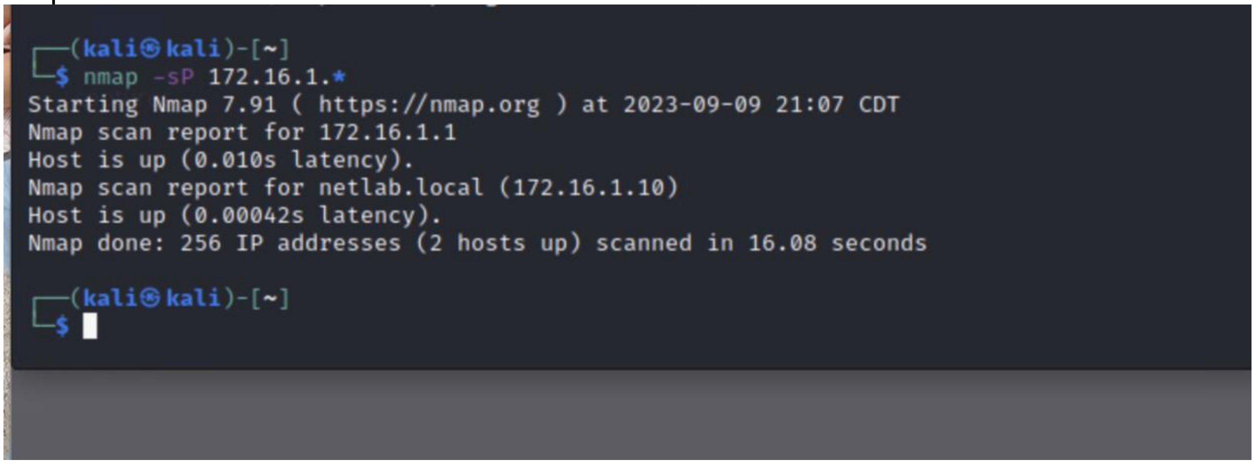
Step 2



```
PS C:\Windows\system32> [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()


Forest                  : netlab.local
DomainControllers       : {WinOS.netlab.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : WinOS.netlab.local
RidRoleOwner            : WinOS.netlab.local
InfrastructureRoleOwner : WinOS.netlab.local
Name                    : netlab.local


PS C:\Windows\system32>
```

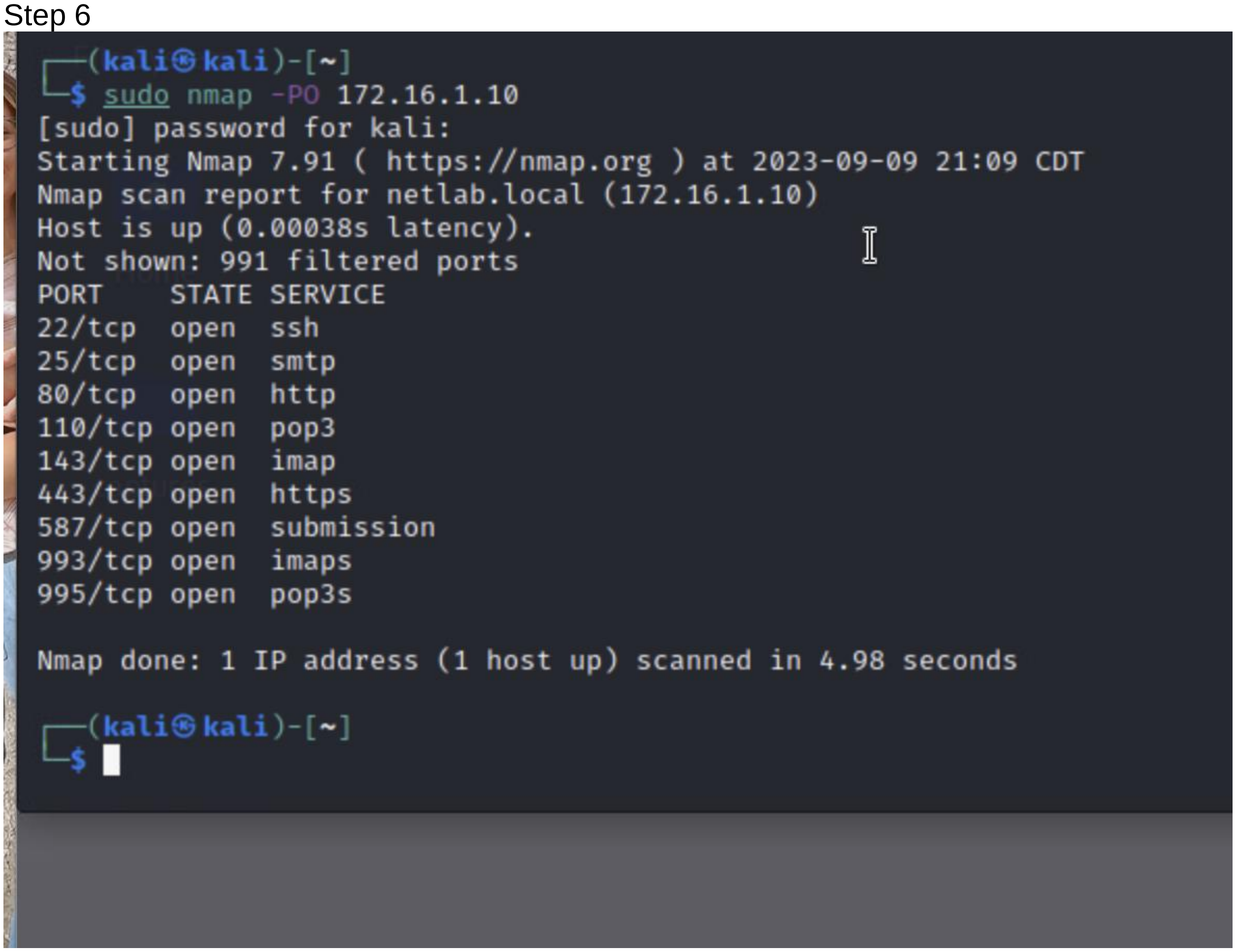
3:

Step 4



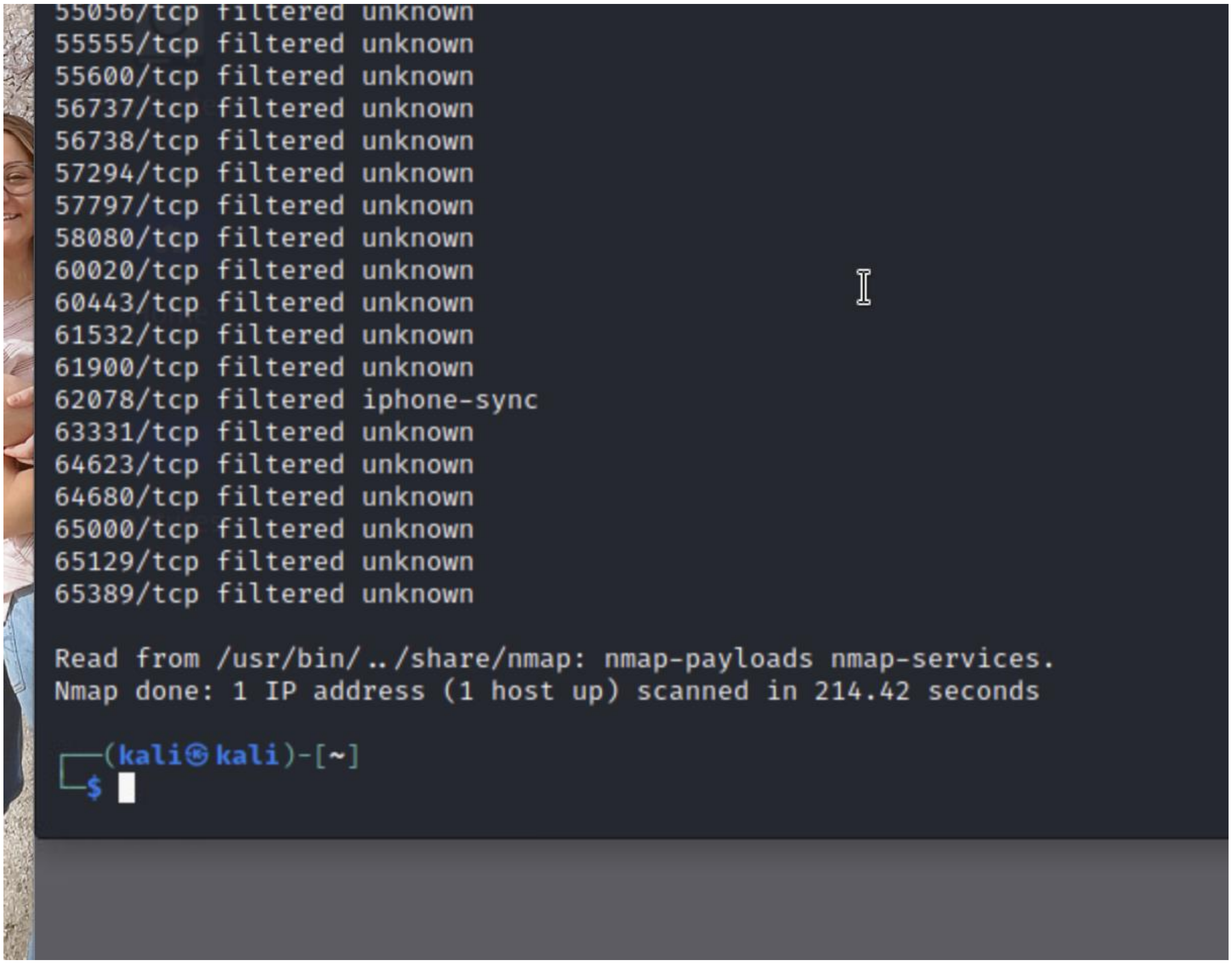
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.*
Starting Nmap 7.91 ( https://nmap.org ) at 2023-09-09 21:07 CDT
Nmap scan report for 172.16.1.1
Host is up (0.010s latency).
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00042s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.08 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Step 6



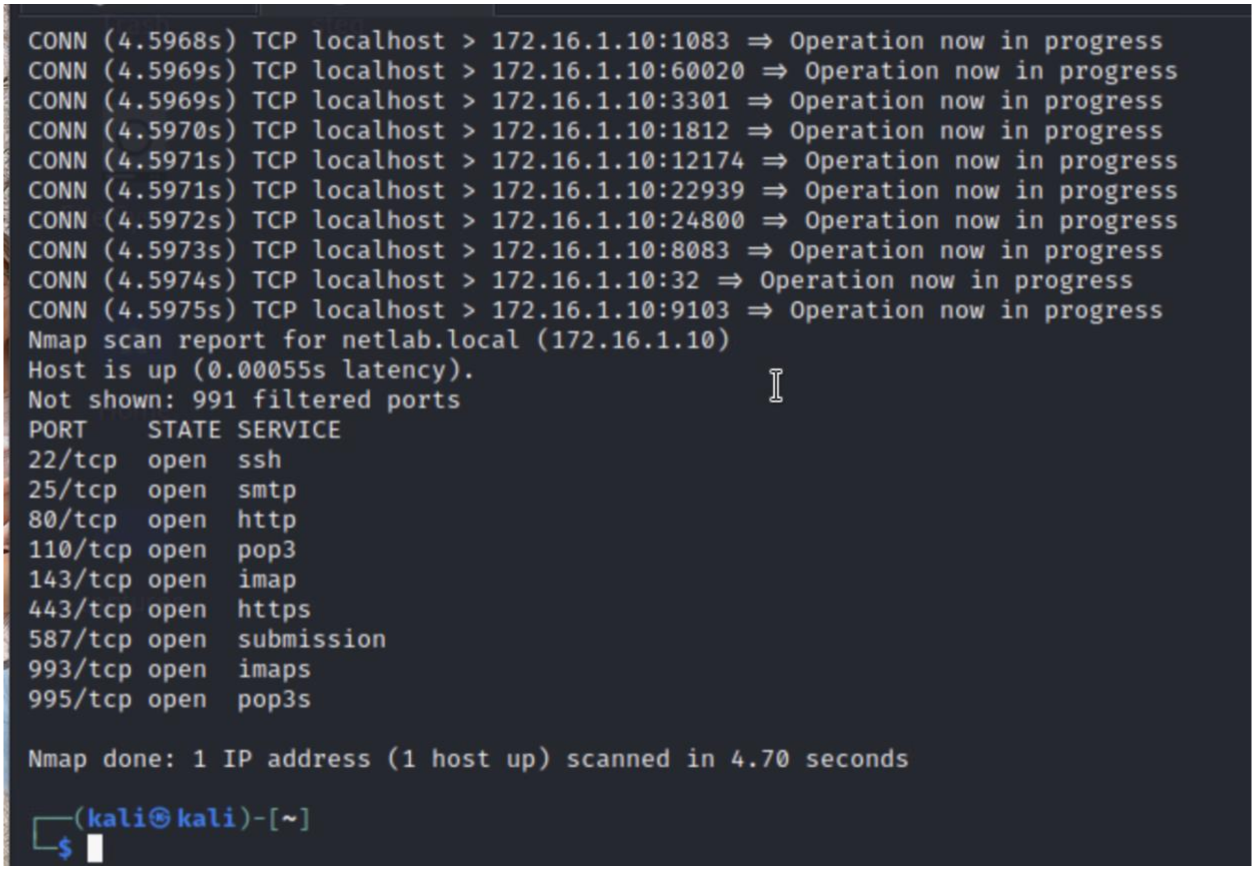
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PO 172.16.1.10
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-09-09 21:09 CDT
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00038s latency).
Not shown: 991 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Step 9



```
55056/tcp filtered unknown
55555/tcp filtered unknown
55600/tcp filtered unknown
56737/tcp filtered unknown
56738/tcp filtered unknown
57294/tcp filtered unknown
57797/tcp filtered unknown
58080/tcp filtered unknown
60020/tcp filtered unknown
60443/tcp filtered unknown
61532/tcp filtered unknown
61900/tcp filtered unknown
62078/tcp filtered iphone-sync
63331/tcp filtered unknown
64623/tcp filtered unknown
64680/tcp filtered unknown
65000/tcp filtered unknown
65129/tcp filtered unknown
65389/tcp filtered unknown

Read from /usr/bin/../share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 214.42 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Step 15



```
CONN (4.5968s) TCP localhost > 172.16.1.10:1083 ⇒ Operation now in progress
CONN (4.5969s) TCP localhost > 172.16.1.10:60020 ⇒ Operation now in progress
CONN (4.5969s) TCP localhost > 172.16.1.10:3301 ⇒ Operation now in progress
CONN (4.5970s) TCP localhost > 172.16.1.10:1812 ⇒ Operation now in progress
CONN (4.5971s) TCP localhost > 172.16.1.10:12174 ⇒ Operation now in progress
CONN (4.5971s) TCP localhost > 172.16.1.10:22939 ⇒ Operation now in progress
CONN (4.5972s) TCP localhost > 172.16.1.10:24800 ⇒ Operation now in progress
CONN (4.5973s) TCP localhost > 172.16.1.10:8083 ⇒ Operation now in progress
CONN (4.5974s) TCP localhost > 172.16.1.10:32 ⇒ Operation now in progress
CONN (4.5975s) TCP localhost > 172.16.1.10:9103 ⇒ Operation now in progress
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00055s latency).
Not shown: 991 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Commentary:

In this lab we used nmap to look into other systems that we can reach. Nmap can tell us a lot about other systems and help probe for possible vulnerabilities. I learned that nmap is super powerful and makes it really easy for hackers to learn information. Knowing this information, companies can use nmap on their own systems to see what hackers can see and be able to patch vulnerabilities before hackers exploit them.