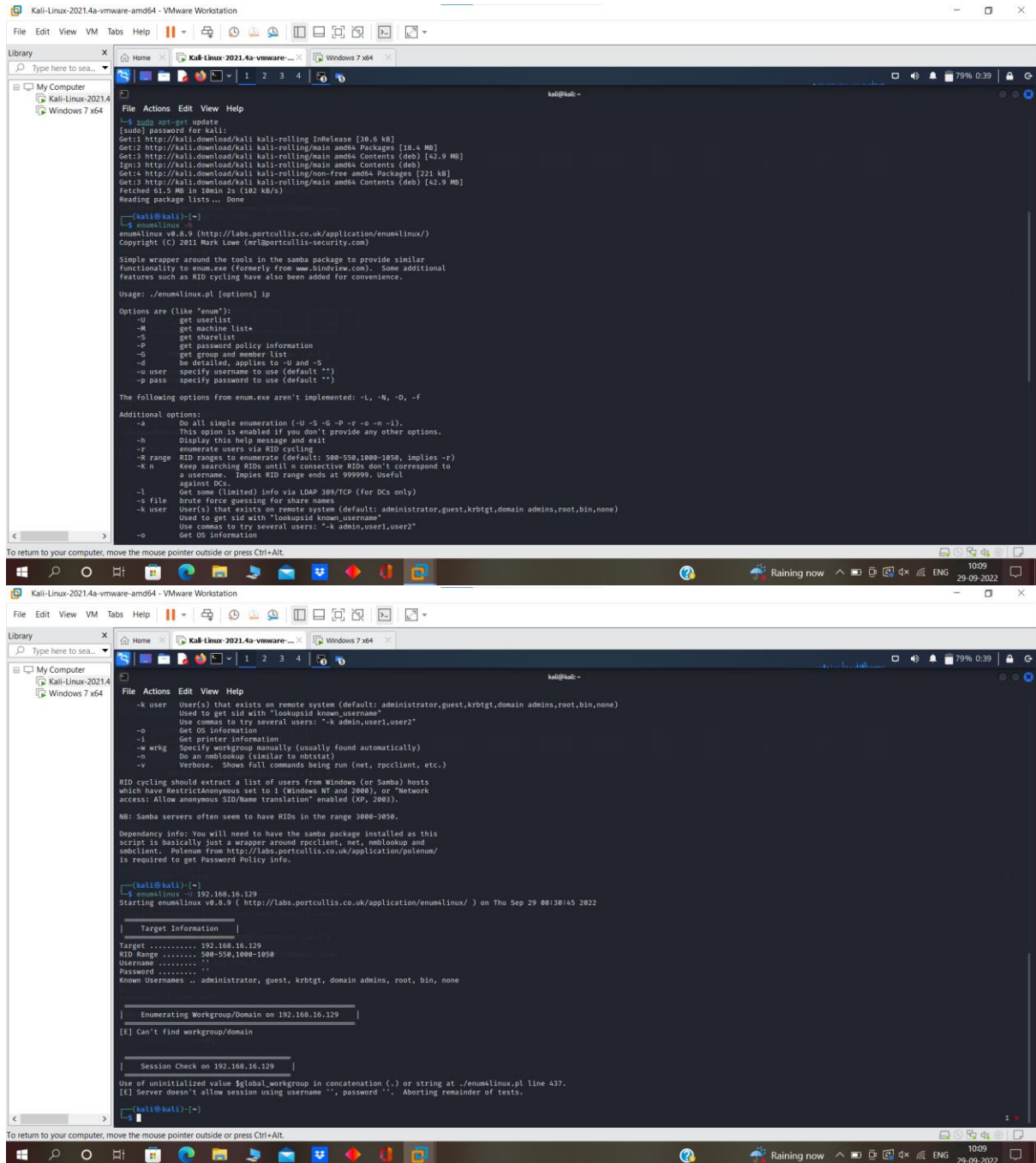


# EXPERIMENT 10:

## OUTPUT:



```
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [38.4 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42.9 MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [221 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42.9 MB]
Fetched 61.9 MB in 19min 2s (192 kB/s)
Reading package lists... Done

[kali@kali:~]$ sudo apt-get update
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
-u get userlist
-m get machine list
-s get sharelist
-P get password policy information
-G get group and member list
-d be detailed, applies to -u and -s
-u user specify username to use (default '')
-p pass specify password to use (default '')

The following options from enum.exe aren't implemented: -L, -M, -D, -f

Additional options:
-a do all simple enumeration (-u -s -G -P -r -o -n -i).
  This option is enabled if you don't provide any other options.
-h Display this help message and exit
-r enumerate users via RID cycling
-R RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-k n keep searching RIDs until n consecutive RIDs don't correspond to
  a username. Implies RID range ends at 999999. Useful
  against DCs.
-l get some (limited) info via LDAP 389/TCP (for DCs only)
-f file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest,krbtgt,admin,root,bin,nome)
  Used to get sid with "lookupsid known_username"
  Use commas to try several users: "-k admin,user1,user2"
  Get OS information
-o OS information
-i Get printer information
-wrkg Specify workgroup manually (usually found automatically)
-n Do an nmblookup (similar to nbtstat)
-v Verbose. Shows full commands being run (net, rpcclient, etc.)

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependency info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient. P01enum from http://labs.portcullis.co.uk/application/p01enum/
is required to get Password Policy info.

[kali@kali:~]$ ./enum4linux.pl 192.168.16.129
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Sep 29 00:30:45 2022

Target Information
Target ..... 192.168.16.129
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 192.168.16.129
[E] Can't find workgroup/domain

Session Check on 192.168.16.129
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

[kali@kali:~]$
```