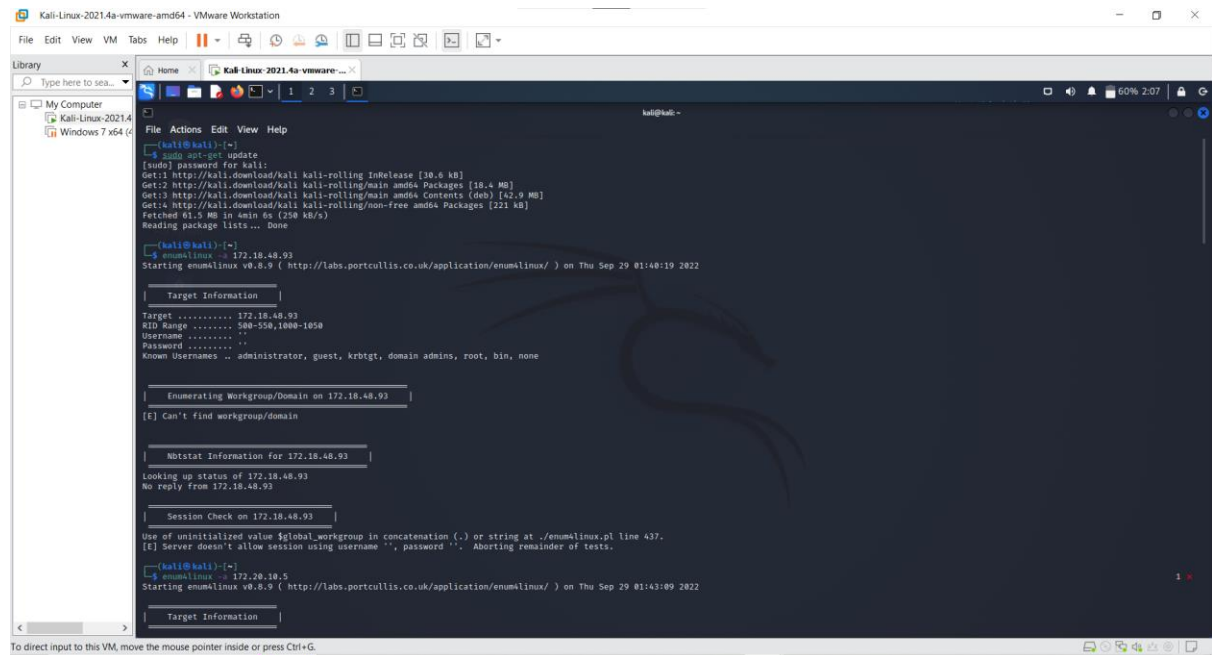


EXPERIMENT 10:

OUTPUT:



```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
Kali Linux 2021.4a-vmware-amd64
File Actions Edit View Help
[kali@kali:~]$ sudo apt-get update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 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]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [221 kB]
Fetched 61.5 MB in 4min 6s (258 kB/s)
Reading package lists... Done
[kali@kali:~]$ enumlinux -i 172.18.48.93
Starting enumlinux v0.8.9 ( http://labs.portcullis.co.uk/application/enumlinux/ ) on Thu Sep 29 01:40:19 2022

Target Information
Target ..... 172.18.48.93
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 172.18.48.93
[E] Can't find workgroup/domain

Nbtstat Information for 172.18.48.93
Looking up status of 172.18.48.93
No reply from 172.18.48.93

Session Check on 172.18.48.93
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enumlinux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
[kali@kali:~]$ enumlinux -i 172.20.10.5
Starting enumlinux v0.8.9 ( http://labs.portcullis.co.uk/application/enumlinux/ ) on Thu Sep 29 01:43:09 2022

Target Information
Target ..... 172.20.10.5
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 172.20.10.5
[E] Can't find workgroup/domain

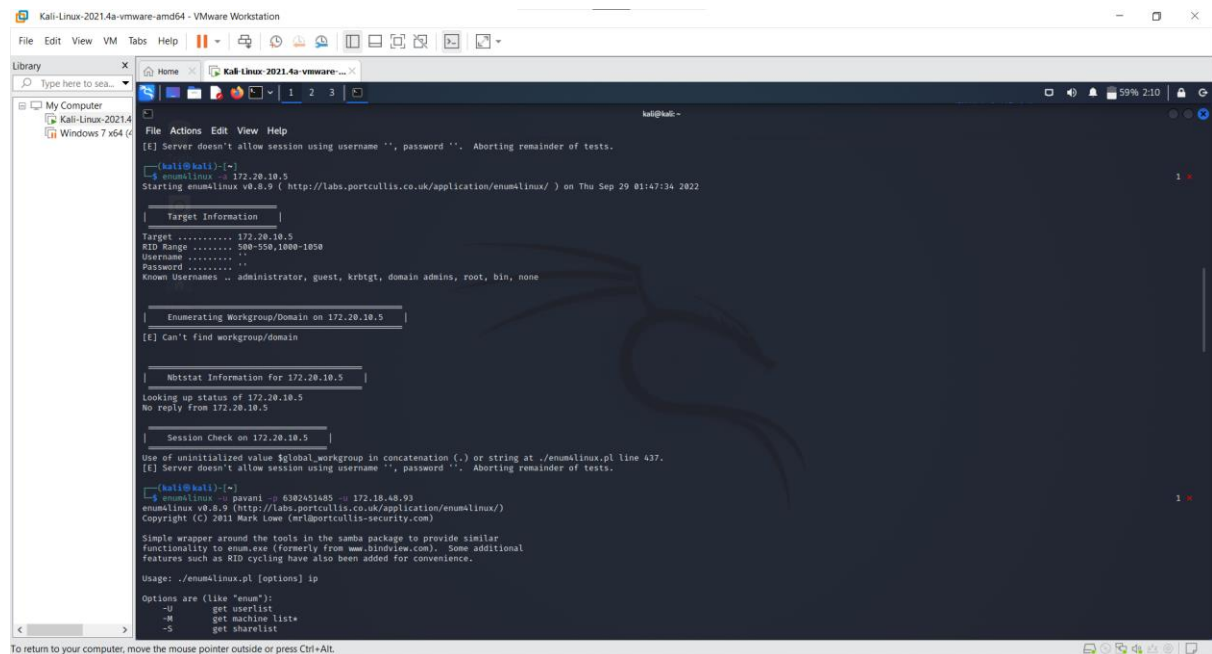
Nbtstat Information for 172.20.10.5
Looking up status of 172.20.10.5
No reply from 172.20.10.5

Session Check on 172.20.10.5
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enumlinux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
[kali@kali:~]$ enumlinux -i pavani -u 6302451485 -i 172.18.48.93
enumlinux v0.8.9 (http://labs.portcullis.co.uk/application/enumlinux/)
Copyright (C) 2011 Mark Lowe (mrld@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: ./enumlinux.pl [options] ip

Options are (like "enum"):
-u get userlist
-m get machine list
-s get sharelist
```



```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
Kali Linux 2021.4a-vmware-amd64
File Actions Edit View Help
[kali@kali:~]$ enumlinux -i 172.20.10.5
Starting enumlinux v0.8.9 ( http://labs.portcullis.co.uk/application/enumlinux/ ) on Thu Sep 29 01:47:34 2022

Target Information
Target ..... 172.20.10.5
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 172.20.10.5
[E] Can't find workgroup/domain

Nbtstat Information for 172.20.10.5
Looking up status of 172.20.10.5
No reply from 172.20.10.5

Session Check on 172.20.10.5
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enumlinux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
[kali@kali:~]$ enumlinux -i pavani -u 6302451485 -i 172.18.48.93
enumlinux v0.8.9 (http://labs.portcullis.co.uk/application/enumlinux/)
Copyright (C) 2011 Mark Lowe (mrld@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: ./enumlinux.pl [options] ip

Options are (like "enum"):
-u get userlist
-m get machine list
-s get sharelist
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
kali@kali: ~
$ ./enumlinux.pl [-c]
enumlinux v0.8.9 (http://labs.portcullis.co.uk/application/enumlinux/)
Copyright (C) 2011 Mark Lowe (mrld@portcullis-security.com)

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

Usage: ./enumlinux.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, -N, -O, -f

Additional options:
-a Do all single enumeration (-U -S -G -P -r -d -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 range 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 99999. Useful
  against DCs.
-l Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest,krbtgt,
  domain admins,root,bin,none)
  Used to get sid data "lookupsid known_username"
  Use commas to try several users: "-k admin,user2"
-o Get OS information
-i Get printer information
-w wrkg Specify workgroup manually (usually found automatically)
-n Do an smblookup (similar to nbstat)
-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.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
kali@kali: ~
-i Get printer information
-w wrkg Specify workgroup manually (usually found automatically)
-n Do an smblookup (similar to nbstat)
-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, smblookup and
smbclient. Penum from http://labs.portcullis.co.uk/application/penum/
is required to get Password Policy info.

[kali@kali:~]$ ./enumlinux 172.18.48.93 -s
Starting enumlinux v0.8.9 ( http://labs.portcullis.co.uk/application/enumlinux/ ) on Thu Sep 29 01:54:01 2022

Target Information
Target ..... 172.18.48.93
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

Enumerating Workgroup/Domain on 172.18.48.93
[E] Can't find workgroup/domain

Nbstat Information for 172.18.48.93
Looking up status of 172.18.48.93
No reply from 172.18.48.93

Session Check on 172.18.48.93
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enumlinux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```