enum4linux

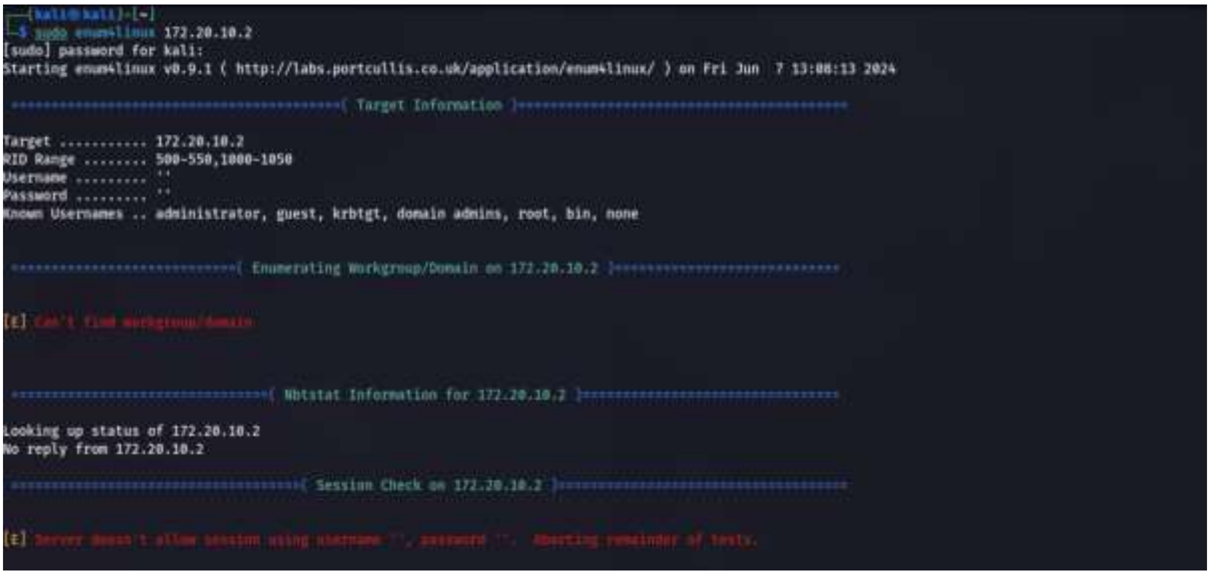
enum4linux is a tool used to gather information from Windows systems using SMB (Server Message Block) protocol. It is often used in penetration testing to enumerate various details about a Windows system, such as user accounts, shares, and other information.

SMB (Server Message Block) is a protocol that allows resources on the same network to share files, browse the network, and print over the network. It was initially used on Windows, but Unix systems can use SMB through Samba.

Typically, there are SMB share drives on a server that can be connected to and used to view or transfer files. SMB can often be a great starting point for an attacker looking to discover sensitive information.

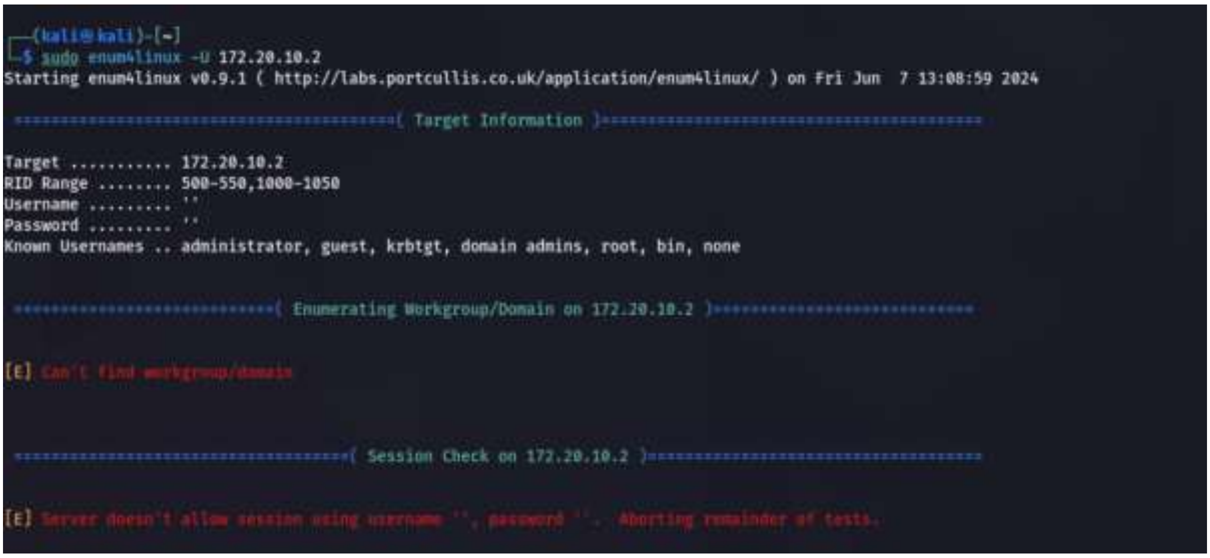
Example: -

1. To perform a basic enumeration use enum4linux command along with target IP.



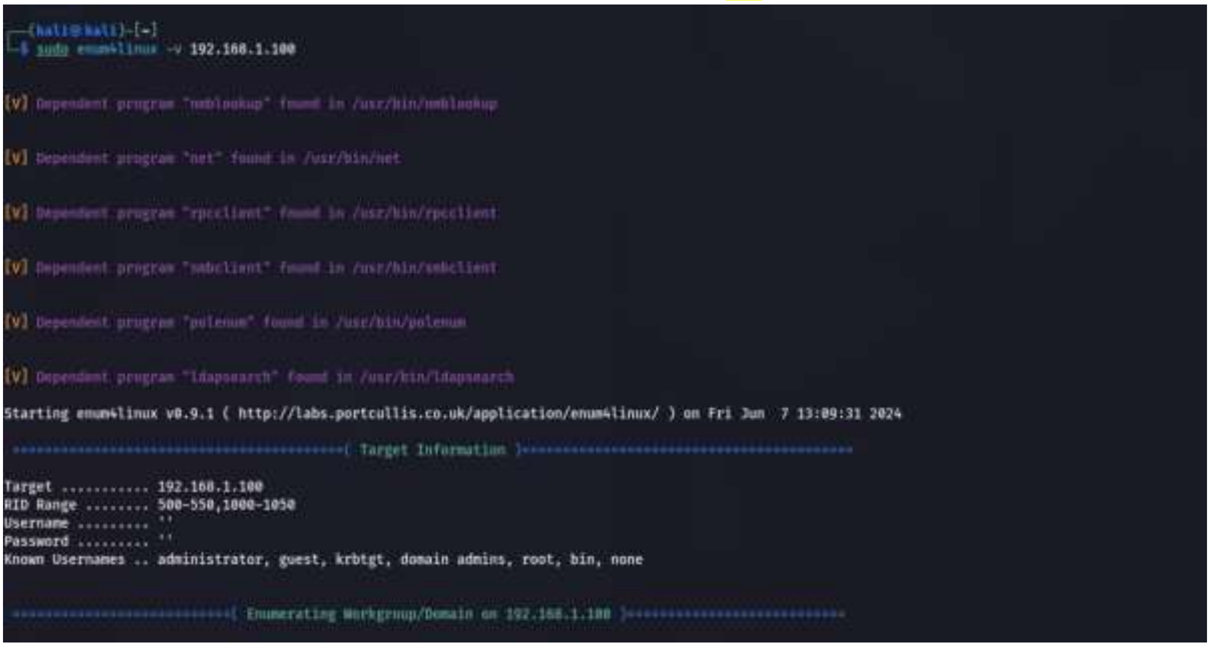
```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux 172.20.10.2
[sudo] password for kali:
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun  7 13:08:13 2024

 =========================================( Target Information )=========================================

Target ........... 172.20.10.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.20.10.2 )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for 172.20.10.2 )================================

Looking up status of 172.20.10.2
No reply from 172.20.10.2

 ====================================( Session Check on 172.20.10.2 )====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

2. To scan for the user we will use -U flag.



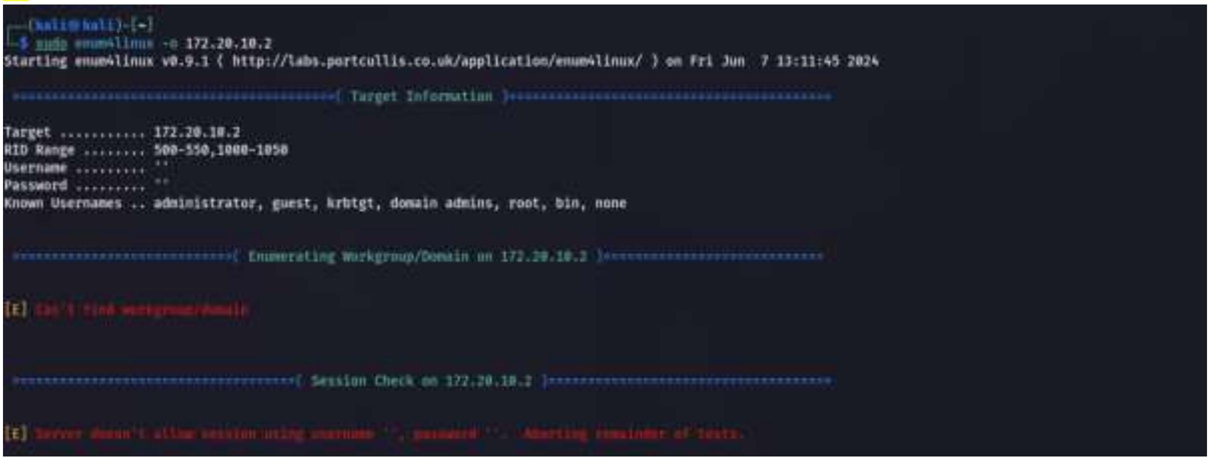
```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux -U 172.20.10.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun  7 13:08:59 2024

 =========================================( Target Information )=========================================

Target ........... 172.20.10.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.20.10.2 )============================


[E] Can't find workgroup/domain



 ====================================( Session Check on 172.20.10.2 )====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

3. To run the scan in verbose mode use -v flag.



```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux -v 192.168.1.100

[V] Dependent program "nmblookup" found in /usr/bin/nmblookup

[V] Dependent program "net" found in /usr/bin/net

[V] Dependent program "rpcclient" found in /usr/bin/rpcclient

[V] Dependent program "smbclient" found in /usr/bin/smbclient

[V] Dependent program "polenum" found in /usr/bin/polenum

[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun  7 13:09:31 2024

 =========================================( Target Information )=========================================

Target ........... 192.168.1.100
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.1.100 )===========================
```

4. To get information related operating system we will use -o flag along with the target IP.



```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux -o 172.20.10.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun  7 13:11:45 2024

 =========================================( Target Information )=========================================

Target ........... 172.20.10.2
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.20.10.2 )============================


[E] Can't find workgroup/domain



 ====================================( Session Check on 172.20.10.2 )====================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```