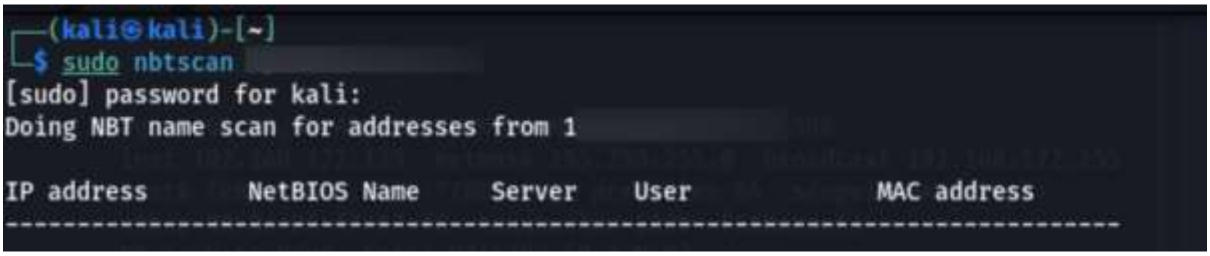
# nbtscan

Nbtscan is an automated cyber-security tool for scanning IP networks for NetBIOS name information. Nbtscan tool sends Net-BIOS status query to each address in supplied range and lists received data in human-readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name, and MAC address (such as Ethernet). Nbtscan tool is available in the apt manager and it’s also available on the internet for free.

nbtscan is a powerful yet simple tool for network scanning and discovering NetBIOS information. With the commands and options provided in this tutorial, you should be able to effectively use nbtscan to gather information about the Windows machines on your network.

# Example: -

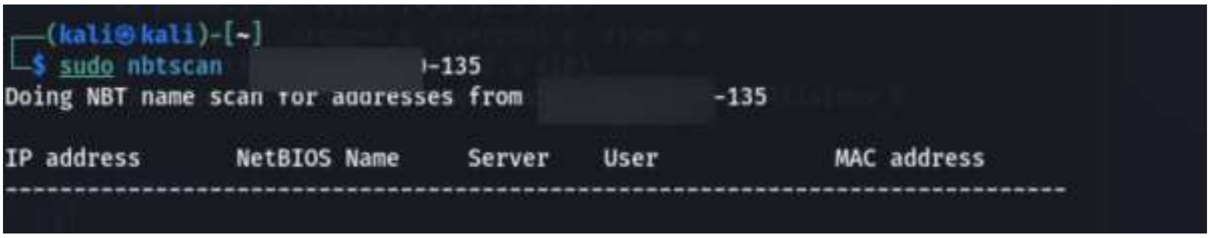
1. For a basic scan use nbtscan with the target IP address.



```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan [redacted]
[sudo] password for kali:
Doing NBT name scan for addresses from 1[redacted]

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
```

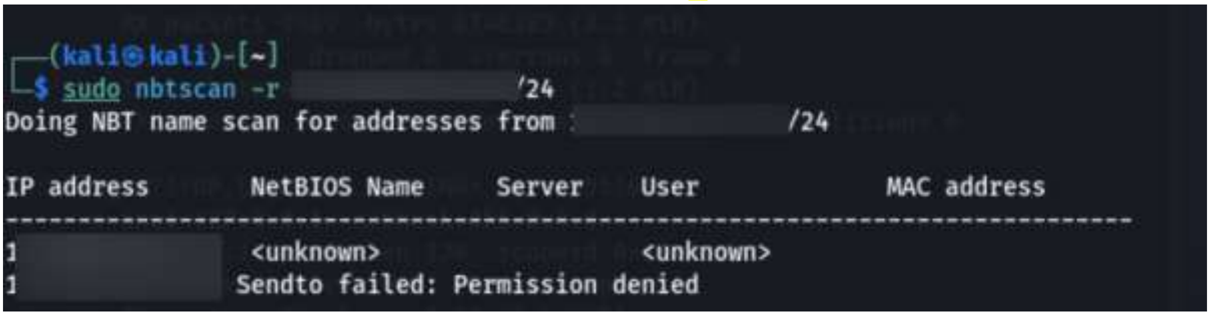
2. To scan for a range of IP address use – in between the target range.



```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan [redacted]-135
Doing NBT name scan for addresses from [redacted]-135

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
```

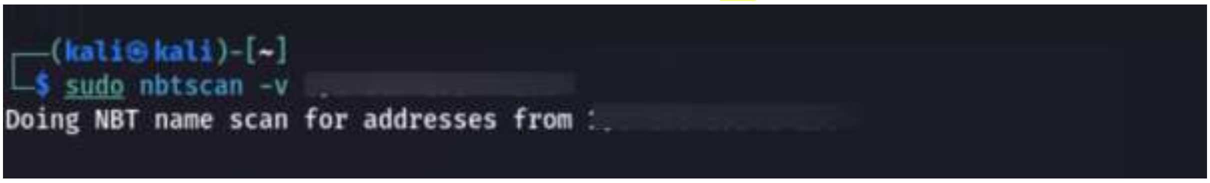
3. To have a scan for subnet CIDR use / with the target IP.



```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan -r [redacted]/24
Doing NBT name scan for addresses from [redacted]/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
1[redacted]      <unknown>                  <unknown>
1[redacted]     Sendto failed: Permission denied
```

4. To have a scan in verbose mode use -v flag.



```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan -v [redacted]
Doing NBT name scan for addresses from [redacted]
```