**netbios-ssn**

**Submitted by:- Binay Chaudhary**

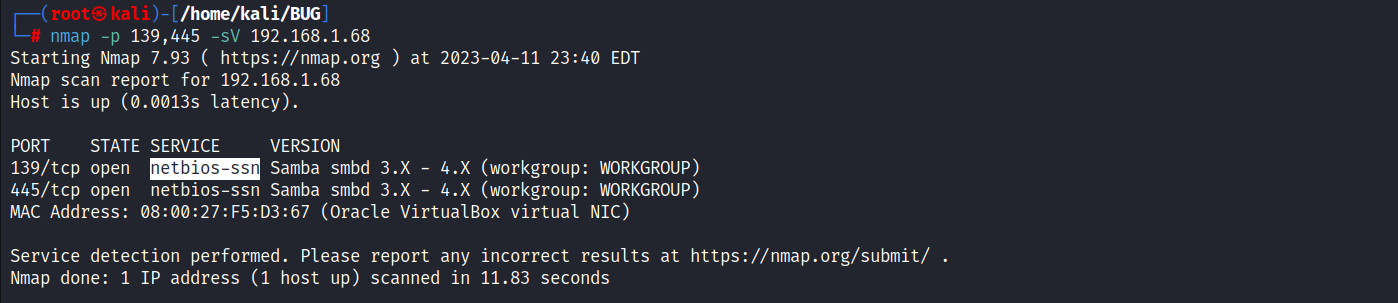
**Submitted to:- Er. Suman Bahadur Basnet**

**Contents page no.**

* **NMAP 3**
* **NmbLookup 4**
* **smbMAP 4**
* **smbClient 5**
* **Consclusion 5**

**NMAP**

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.



Here, in this above picture we’ve found that the port 139, 445 are open and then, we’ve found the version and the service of the port. And we can now exploit through the open port.

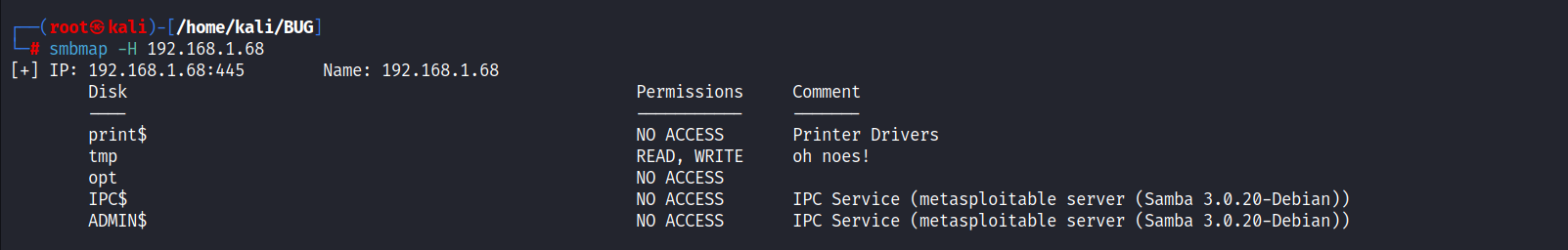
**Nmblookup**

Here, we have found that the machine name and the workgroup of the company printer

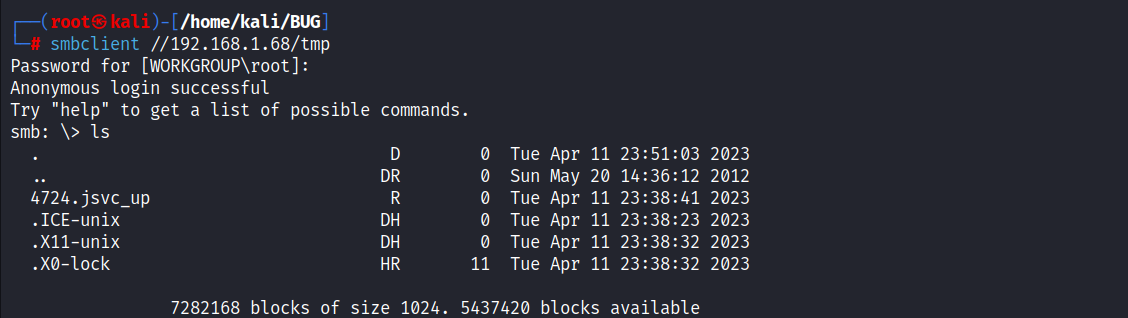


**smbMAP**

Here, we can see that we can easily get access to it without the password and now we can easily access the tmp that device has read and write permission.



**Smbclient**

****Here, we can see that this file has not any password due to the misconfiguration of the group we can easily access to the tmp folder.

So, let’s try to view the file.

Conclusion

* Here, we have to change the weak credentials to strong password that an attacker can’t get access.
* We, have to make sure that the password should be there when the attacker wants to get access through the port 139, 445.