ETHICAL HACKING
LAB SERIES

Lab 8: Enumerating SMB with enum4linux

Material in this Lab Aligns to the Following Certification Domains/Objectives		
Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
4: Enumeration	12: Privilege Escalation	4: Enumerating Users

Document Version: 2016-03-09

Contents

Introduction

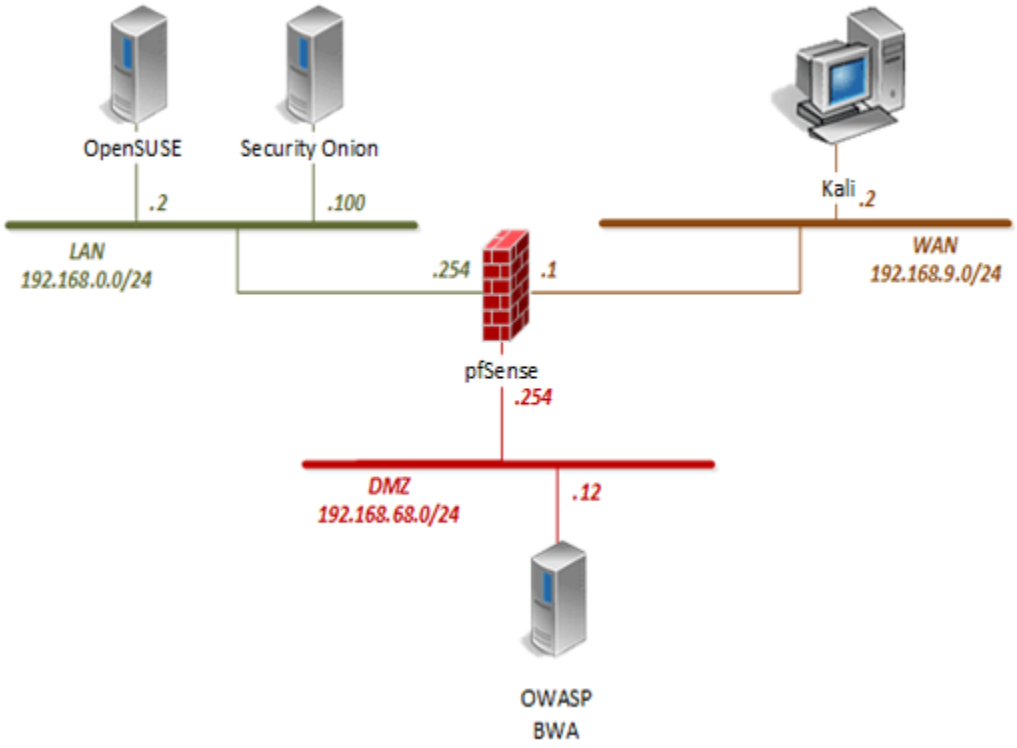
NetBIOS is a commonly attacked program on Windows machines, however, Linux servers with a SAMBA installed also use NetBIOS. This lab addresses the vulnerabilities of NetBIOS and how to exploit them.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Enumerating the Samba Server with enum4linux
2. Cracking Samba Users with xHydra

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Enumerating the Samba Server with enum4linux

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.

6. In the new *Terminal* window, type the command below to view the available options for the *enum4linux* application. Press **Enter**.

```
enum4linux -h
```

7. Initiate *enum4linux* against the *OWASP* VM. Identify the target OS type by typing the command below followed by pressing the **Enter** key.

```
enum4linux -o 192.168.68.12
```

```
 =========================================
|    OS information on 192.168.68.12    |
 =========================================
[+] Got OS info for 192.168.68.12 from smbclient: Domain=[WORKGROUP] OS=[Unix] S
erver=[Samba 3.4.7]
[+] Got OS info for 192.168.68.12 from srvinfo:
        OWASPBWA       Wk Sv PrQ Unx NT SNT owaspbwa server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x809a03
enum4linux complete on Fri Dec 18 10:55:00 2015
```

Notice *enum4linux* helps us identify the target running a Samba server.

8. Since *OWASP* is running a Samba server, enter the command below to try to enumerate its shares.

```
enum4linux -S 192.168.68.12
```

```
 ==========================================
|    Share Enumeration on 192.168.68.12    |
 ==========================================
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        apache          Disk      Apache Web Server Root
        tomcat          Disk      Tomcat6 Root
        var             Disk      /var
        etc             Disk      /etc
        usr             Disk      /usr
        owaspbwa        Disk      /owaspbwa
        IPC$            IPC       IPC Service (owaspbwa server (Samba, Ubuntu))

        Server               Comment
        ---------            -------
        OWASPBWA             owaspbwa server (Samba, Ubuntu)

        Workgroup            Master
        ---------            -------
        WORKGROUP            OWASPBWA
```

Notice several shares are listed; one of which is IPC$.

9. Try to connect to the null share using the *smbclient* command. This is equivalent to the *net use* command in *Windows*. Type the command below followed by pressing the **Enter** key.

```
smbclient -I 192.168.68.12 -L IPC$ -N -U "”
```

```
root@Kali2:~# smbclient -I 192.168.68.12 -L IPC$ -N -U ""
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        apache          Disk      Apache Web Server Root
        tomcat          Disk      Tomcat6 Root
        var             Disk      /var
        etc             Disk      /etc
        usr             Disk      /usr
        owaspbwa        Disk      /owaspbwa
        IPC$            IPC       IPC Service (owaspbwa server (Samba, Ubuntu))
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]

        Server               Comment
        ---------            -------
        OWASPBWA             owaspbwa server (Samba, Ubuntu)

        Workgroup            Master
        ---------            -------
        WORKGROUP            OWASPBWA
```


Notice the successful enumeration of the "null share" with no username or password.

10. Enter the command below in an attempt to retrieve the user list on the system.

```
enum4linux -U 192.168.68.12
```

```
 ==============================
|    Users on 192.168.68.12    |
 ==============================
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody   Name: nobody    Desc:
index: 0x2 RID: 0x3e8 acb: 0x00000010 Account: user     Name: user,,,   Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: root     Name: root      Desc:

user:[nobody] rid:[0x1f5]
user:[user] rid:[0x3e8]
user:[root] rid:[0x3e9]
enum4linux complete on Fri Dec 18 11:56:52 2015
```

Notice the three users listed back along with their respective *Relative Identifier (RID)* numbers.

11. Convert the *RIDs* from the given hexadecimal to decimal.

User	Hexadecimal	Decimal
nobody	0x1f5	501
user	0x3e8	1000
root	0x3e9	1001

Notice the numbering, for example, the "nobody" user has a 501 RID converted to decimal which in *Windows* is an "Administrator" account while "root has a 1001 which is a normal "user" account in *Windows*.

12. Enter the command below to check the password policy on the server.

```
enum4linux -P 192.168.68.12
```

Notice the only policy is a minimum password length of 5 and a 30-minute lockout.

13. Try to obtain login information by generating a dictionary based off the server's site. Since passwords are a minimum of 5 characters, that will be used as a basis for the wordlist generation. Enter the command below.

```
cewl 192.168.68.12 -m 5 -w wordlist
```

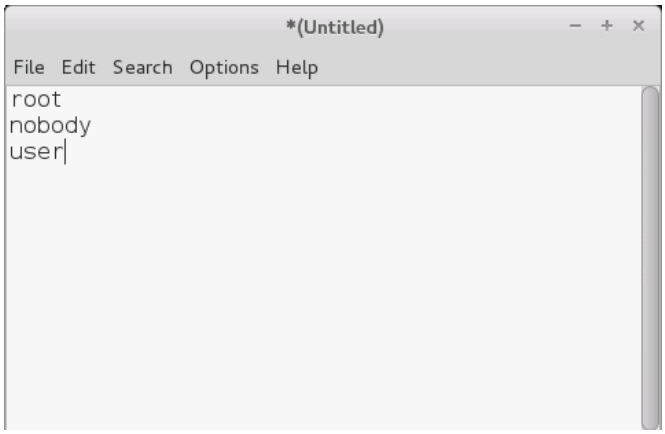

14. Once the prompt appears, observe the contents of the new wordlist file. Enter the command below.

```
cat wordlist | less
```

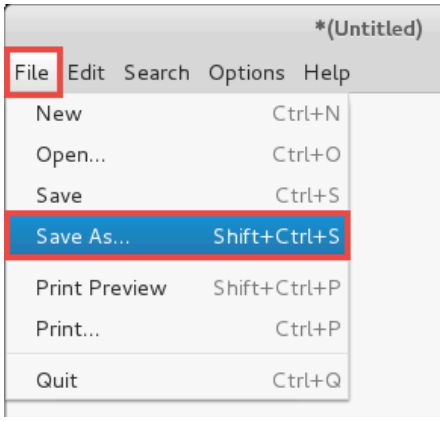
Press the **Spacebar** to skip to the next page or the **Enter** key to skip by each line. Press **Q** to quit at any given time and to receive the prompt back.

15. Open the *Leafpad* application by clicking on the **Leafpad** icon located on the left panel.

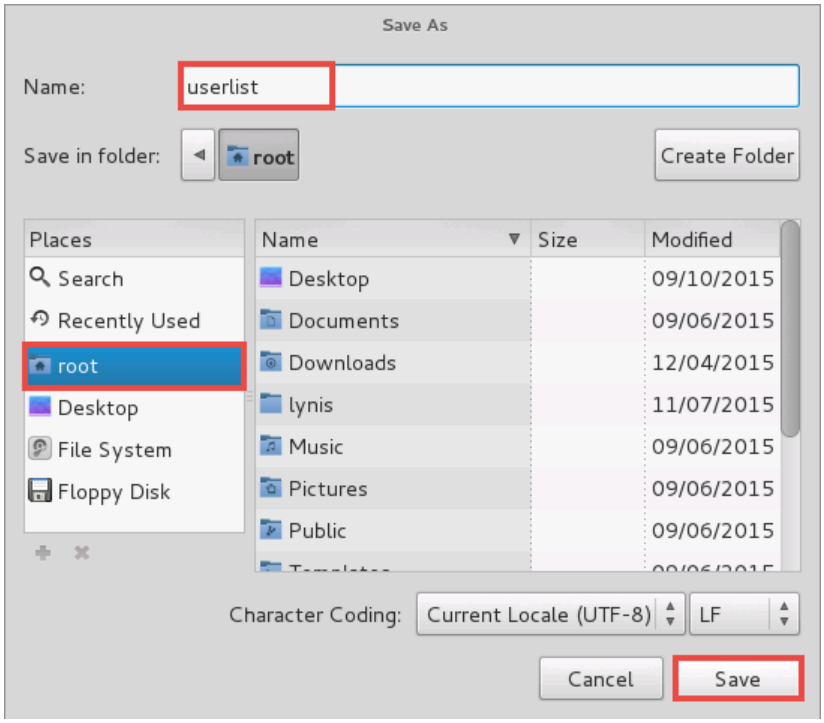
16. Create a *userlist* file containing the three users found on the Samba server. Type **`root`**, **`nobody`**, and **`user`** with each user being separated by each line like shown below.



17. Save the *userlist* file by selecting **File > Save As**.



18. In the *Save As* window, select the **root** directory in the *Places* panel. Type `userlist` in the *Name* text field and click **Save**.

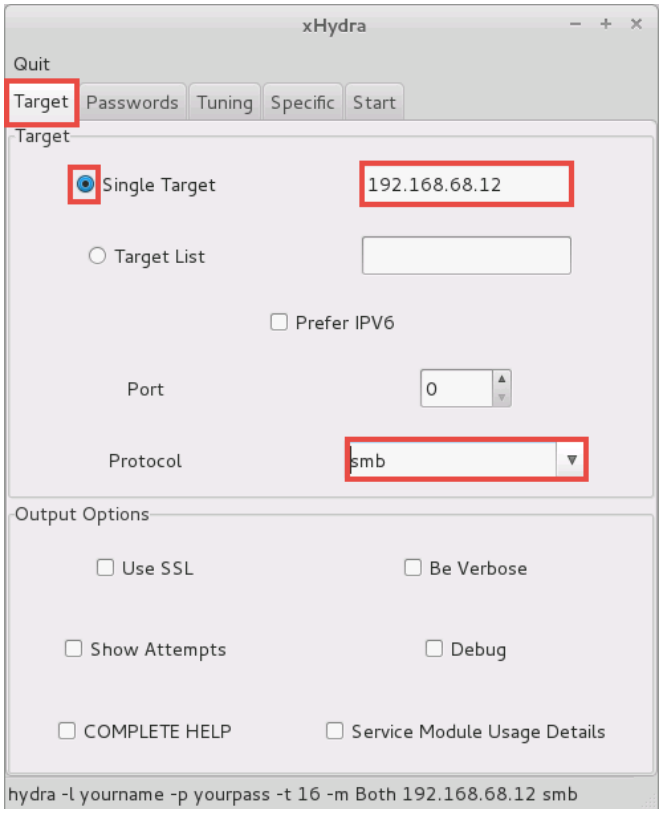


2 Cracking Samba Users with xHydra

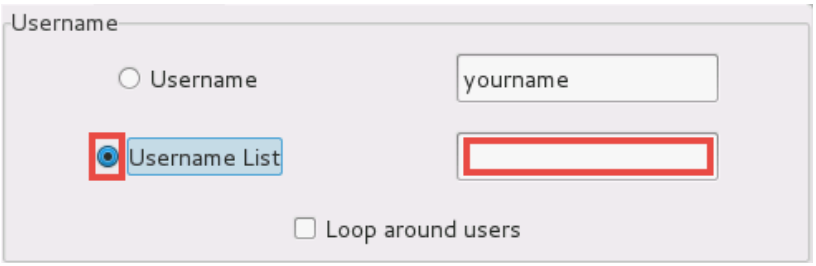
1. Navigate back to the **Terminal** window.
2. Launch the **xhydra** application by typing the command below followed by pressing the **Enter** key.

```
xhydra
```

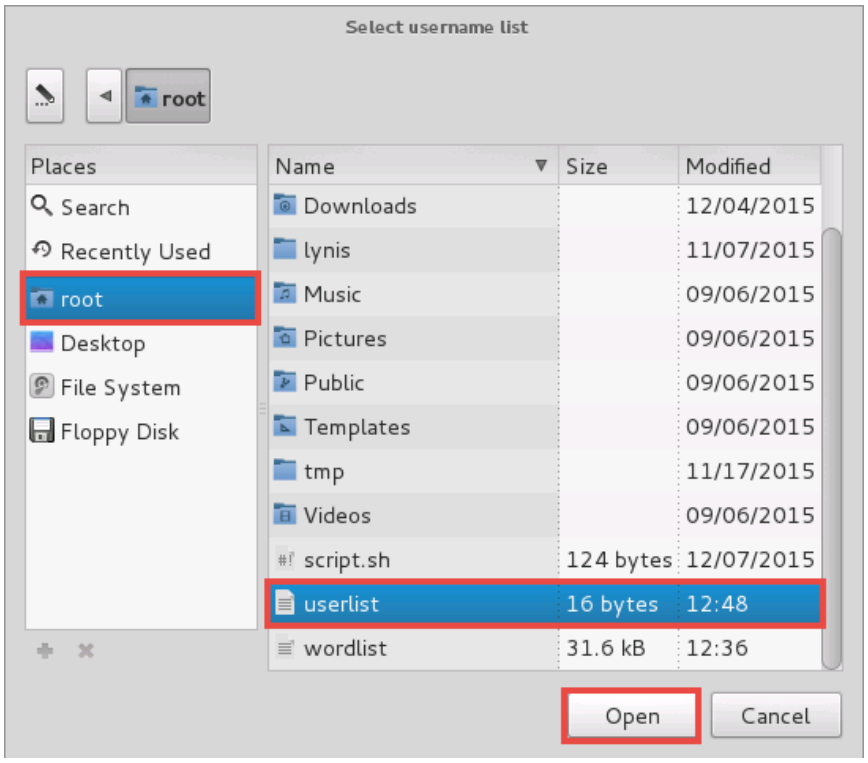
3. Notice a new *xHydra* window appears. While viewing the **Target** tab, enter `192.168.68.12` as a *Single Target IP* address.
4. Select **smb** from the *Protocol* drop-down menu.



5. Click the **Passwords** tab.
6. Select the Username List radio button and click within the white space in its text field.



7. Notice a *Select username list* window appears, click the **root** directory and select the **userlist** file. Click **Open**.



8. While viewing the *Passwords* tab on the *xHydra* window, select the **Password List** radio button and click within the white space in its text field.

9. Notice a *Select password list* window appears, click the **root** directory and select the **wordlist** file. Click **Open**.
10. Click the **Start** tab.
11. Click the **Start** button located towards the bottom of the *xHydra* window.

12. Notice the successful attempt in cracking the *root* and *user* accounts' passwords.

```
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[445][smb] host: 192.168.68.12   login: root   password: [illegible]
[STATUS] 4843.00 tries/min, 4843 tries in 00:01h, 5543 todo in 00:02h, 1 active
[STATUS] 3229.50 tries/min, 6459 tries in 00:02h, 3927 todo in 00:02h, 1 active
[445][smb] host: 192.168.68.12   login: user   password: [illegible]
<finished>
```

13. Close the **Kali** PC viewer.

