# Overview

## Goals

This lab is intended to showcase some network auditing techniques including network scanning, SNMP enumeration, man in the middle attacks and traffic sniffing. By the end if this lab you should have a good idea how people may attack a network as well as what to do to protect it.

Deliverables

* A lab report including the following:
  + Description of the lab steps completed and the results.
  + Filled information section

## Information

|  |  |  |
| --- | --- | --- |
| ***Description*** | ***Used in Lab*** | ***Value*** |
| NetAudit VM IP Address | **NETAUDIP** |  |
| NetAudit VM MAC Address | **NETAUDMAC** |  |
| Other VM IP Address | **OTHER\_IP** |  |
| Other VM MAC Address | **OTHER\_MAC** |  |

## Dealing with long output from commands

Many of the commands you will be running in this lab generate large amounts of output. There are several ways to handle long output, depending on your needs

### Piping output to less

$ cat /proc/cpuinfo | less

### Redirecting output to a file

$ cat /proc/cpuinfo > cpus.txt

# Setup

## Downloading the “victim” VM

Navigate to http://lab302-web.hades.lab/itis3110 in the lab using a web browser. In the *bee-box* directory download the *beebox\_v1.5.7z* to the /scratch/$USER directory on your host workstation. The target VM for this lab is bee-box.

## Starting Virtual Machines

The virtual machine will need to be decompressed. Right-clicking a virtual machine will bring up a context menu. Select the ‘Extract to here’ option for both virtual machines **NOTE: Make sure you wait until extraction is finished before launching the VM**. Each extracted virtual machine is a VMWare VM. Create this VM the same way you did the MorningCatch VM.

Note: When you uncompress the .7z file there are instructions in the INSTALL.txt file. This includes credentials for the system.

## Setting up Kali Linux on the Raspberry Pi

The OS that you will audit from is Kali Linux, a Linux distribution designed for penetration testing. It is an updated version of BackTrack with more tools. An 8GB or larger SD card is required. You will want the fastest SD card available.

Steps to create the Kali image on an SD card using a Linux workstation (your Debian VM image, as you will need root authority):

1. Get a copy of Kali (e.g. kali-1.0.9-rpi.img.xz) from <http://lab302-web.hades.lab/kali-pi>
   1. You will need to unzip the .xz image
   2. Note: a larger unzipped .img is also available. Your choice…
2. Plug your 8GB or larger SD card into a USB SD card adapter
   1. Find the device name for the SD card
      1. df –h
      2. you should see a list of devices starting with /dev/
      3. the disk devices are typically sdXN
         1. X denotes the device (usually starting with *a*)
            1. *a* is usually the first drive that was installed on the workstation
         2. N is a number denoting the partition on that device (usually starting with 1)
            1. The numbers need not be contiguous
      4. The SD card will probably be the “largest” letter
   2. Use dd to copy the .img file to the SD card
      1. dd if=kali.img of=/dev/sdf bs=4M
         1. the if reference should be the name of your Kali image
         2. the of should be the your SD card device
            1. Caution: Do not include any numbers for the SD card device name
         3. Warning: the dd command will destroy all data on the SD card
3. Resize your Kali partition (optional)
   1. The SD card should have 2 partitions, a small boot partition and the main Kali partition.
      1. The Kali partition willl be just over 4GB, and will not be large enough to add many more programs or utilities
   2. Use a tool like gparted to increase the Kali partition to 8GB or larger.
4. Unmount the SD card, plug it into your Pi and boot the Pi.
   1. Log in: UID is root, PW is toor

## Passwords for the VMs

### NETAUDIT VM

Credentials are documented for bee-box in the INSTALL.txt file

### Kali

Username: root Password: toor

## Configuring Kali Linux

Ensure the Pi has a valid lab address.

Check Pi date and time and update if necessary.

# Network Audit

## Determining IP and MAC Addresses of NETAUDIT VM

On your NETAUDIT VM, determine your IP and MAC addresses with the following command:

$ /sbin/ifconfig

Record the IP and MAC addresses in the Information table at the beginning of this document. You will target this IP address when auditing and will use the MAC address for ARP spoofing.

## Scanning the Network

Next, you should scan the lab network. Scan the network with and without pinging hosts first. Your lab report should note the number of hosts you found on line, if you found more hosts when you skipped the ping sweep, and time difference between the scans, if you noticed one.

To run a SYN scan on the lab network:

# nmap –sS 172.16.1.1-254

To run a SYN scan without pinging hosts first:

# nmap –sS –P0 172.16.1.1-254

**Hin**t: what command was used in 2110 to time programs?

## Scanning your NETAUDIT VM

We are going to scan your NETAUDIT VM more in-depth. You will need to take notes on what ports are open because you will be comparing results later.

# nmap –sS –A NETAUDIP

## Walking the SNMP trees

Since we know that this system has SNMP, we should browse through the SNMP trees, both public and private. We are trying to find a “backdoor” planted in the SNMP subsystem. Meditate on why “backdoor” is in quotes, if you are having problems finding it.

SNMP will need to be installed on the Kali Linuxto have access to the snmp tools:

1. If you have internet access:
   1. apt-get update
   2. apt-get install snmp
2. If in the lab
   1. Download SMNP from [http://lab302-web.hades.lab/](http://master.hades.lab/)
   2. Unzip the file (tar –xjf filename)
   3. Change directory to smtp-kali-armel
   4. Run dpkg –i \*

Scan the NETAUDIT system:

# snmpwalk –c public NETAUDIP –v1 1.3.6.1.2.1

# snmpwalk –c public NETAUDIP –v1 1.3.6.1.4.1

## Re-scanning your NETAUDIT VM

You should now rescan your NetAudit VMwith nmap to see if anything has changed.

## Shellshock

The NetAudit VM should be vulnerable to the Shellshock (Bashdoor) attack. To check for vulnerability open a terminal and enter in the shell:

env x='() { :;}; echo vulnerable' bash -c "echo this is a test"

If the word vulnerable is seen this shell has the vulnerability. Document the result.

On your VM and the workstation try the following 3 commands:

env x='() { :;}; /usr/bin/eject' bash -c "echo this is a test"

env x='() { :;}; /usr/bin/eject dvd1' bash -c "echo this is a test"

env x='() { :;}; /usr/bin/eject –T dvd1' bash -c "echo this is a test"

Run the 3rd command 3 or 4 times.

Document the results.

Note: the shellshock vulnerability may be fixed on your workstations this semester. Document if it was fixed and what happens now. Otherwise documents the vulnerability.

## Starting another VM for ARP spoofing

You need to start another virtual machine for the ARP spoofing steps. The VM you use does not matter, as we only want to use an FTP client. Follow the instructions earlier in this lab to find your VM’s IP and MAC addresses and record them in the table at the beginning of this lab.

## Starting Graphics in Kali

We want to use ettercap’s graphics mode so we need to bring up BackTrack’s graphics environment by typing the command below.

# startx

## Starting Ettercap

The Start Menu at the bottom of the screen has a Quick Launch icon for a Terminal (Konsole). Click on it to bring up a terminal and launch ettercap using the command below:

# ettercap –G

## Setting up Ettercap

Ettercap is powerful but complicated. It is extremely easy to configure it incorrectly and take out the entire network. Be care when using it.

* Open the ‘Sniff’ menu and select ‘Unified Sniffing…’
  + You want to sniff on ‘Network Interface eth0’
* Open the ‘Hosts’ menu and select ‘Scan for hosts’
* Open the ‘Hosts’ menu and select ‘Host list’
  + Select your NETAUDIT VM IP and click ‘Add to Target 1’
  + Select your other VM IP and click ‘Add to Target 2’
  + Verify that the MAC addresses match the ones you recorded
* Open the ‘Start’ menu and select ‘Start Sniffing’
* Open the ‘Mitm’ menu and select ‘Arp Poisoning…”
  + Leave the options unchecked

Check that Ettercap log has said ‘Starting Unified sniffing…’ and ‘ARP poisoning victims:’ with one host in group 1 and group 2.

## Testing password sniffing

Now that Ettercap is sniffing the traffic between your two machines you want to test to see if you can sniff passwords. Try FTPing into your NETAUDIT VM from your other VM as root using the NETAUDIT VM password. It is likely that the login will fail but the username and password should show up in ettercap.

$ ftp root@NETAUDIP

## Finishing Up

At your option, you can also remove your NETAUDIT VM.