Honeytables

Introduction and/or Background

One type of honeypot is a honeytoken. A honeytoken is an artifact that is designed to be attractive to an attacker exfiltrating data from a network, but not accessed by anyone who is a legitimate user of the network.

A honeytoken is a form of honeypot, but instead of a server, a honeytoken is a file, login credentials, database table (sometimes referred to as a honeytable), credit card information, or anything else that looks like a real file but is not. That is the critical part of a honeytoken–it has to accurately reflect what the attacker would expect to find on the network, but not be real data.

Objectives

In this project/lab the student will:

- Gain familiarity with honeytables

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

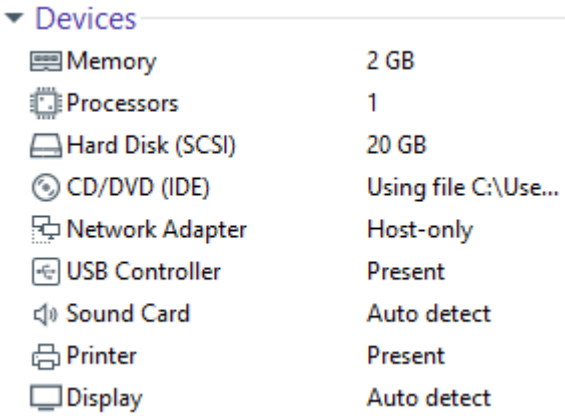
Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Preparation, if not previously installed

0.a apt-get install wireshark –y
0.b apt-get install tcpdump –y

Power off the VMSVR2, change its Network Adapter to Host-Only, and turn it back on.



Open a terminal on VMSVR2 and switch to the root account.

Discover VMSVR2 internet port name and address. Ex output:

ens33, 192.168.115.133

Create a Honeypot as detailed in
http://www.hackerfactor.com/blog/index.php?/archives/841-Building-a-Basic-Honeypot.html

Drop all outgoing traffic:

0.c iptables –A OUTPUT –o <adapter name> –j DROP

From the root account, examine the basic command:

0.d tcpdump -tttt -q -l -i <adapter name> -n -s0

Note: VMSVR2 may be using an adapter different than ens33. It can be displayed by entering the "ip addr" command.

0.e Create a baseline by filtering standard network traffic

e.i Which ports and protocols are actively communicating on the network?

i.1 Arp
i.2 Dns (53)
i.3 192.168.115.255/32
i.4 224.0.0.0/24
i.5 239.0.0.0/8
i.6 255.255.255.255/32
i.7 Fe80::/16

(note these are representative, yours entries may vary.)

e.ii Modify the tcpdump command to filter each normal port, address, and protocol.
tcpdump –tttt –q –l –i <adapter name> –n –s0 not arp and not port 53 and not port 68 and not net 192.168.115.255/32 and not net 224.0.0.0/24 and not net 239.0.0.0/8 and not net 255.255.255.255/32 and not net fe80::/16 and not ff02::/16

e.iii Repeat until nothing is detected.

Ping the VMSVR2 IPv4 address from the ParrotSec VM (these should fail).

Take a screenshot of VMSVR2 ping alert messages.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing Debian's ping alert messages (100 points)	