

Detecting Vmwares Remotely
Guerrilla Strategy

Aditya K Sood
Handle : ZeroKnock

Zknk Den

Abstract

We know vmwares are the best choice of hackers and security professionals now a days. Its very necessary to hit a difference between a normal operating system or a VMware Machine. Its very crucial to emanipate the barriers between the Real Operating systems and virtual ones. Here I am presenting you with a way out to remotely distinguish between machines.

Proof Of Concept

First of I want to tell you I am not going to explain the basics of networking about the protocol arp. I will be direct in applying the concept. This stuff is entirely based on the Arp caching. One must know the exact way for the execution of this process. If you won't forget about Nemesis which uses cache poisoning. But this concept is based on fusion of standard knowledge and Dynamic testing.

I am laying out the practical way from my system. Setting machine to perform penetration analysis.

Check I have Host only networking set on my development Machine.

IP Address MachineA ---- 10.1.1.2
Vmware Machine ---- 10.1.1.1

Why Host Only Networking is chosen.

Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual Ethernet adapter that is visible to the host operating system. This approach can be useful if you need to set up an isolated virtual network. If you use host-only networking, your virtual machine and the host virtual adapter are connected to a private TCP/IP network. Addresses on this network are provided by the VMware DHCP server.

Our Guerilla Strategy based on standard enumeration of networks. In the Web penetration or system testing one should know how to undertake the scanning and related issues so that with minimum penetrated stuff you extract the maximum.

VMWARE Analysis:

MAC Address Analysis:- Vmware provides Three set of standard MAC addresses

MAC Address :48 Bit

Example:- 0x-0x-0x-0x-0x-0x

A-B-C-D-E-F

A+B+C+D+E+F = 8+8+8+8+8+8 = 48 Bits



According To Vmware Designed the A , B , C are standard sets i.e. Vmware Mac addresses start with first three standard codes. These codes are standardly defined and is work in that way.

First Set Of Address:

00-05-69 (hex) VMWARE, Inc.
000569 (base 16) VMWARE, Inc.
3145 Porter Dr., Bldg. F
Palo Alto CA 94304

The first standard VmWare code with starting MAC address **00-05-69-xx-xx-xx** So We Get to one specific knowledge inference about the initial code of the address.

Second Set Of Address:

00-0C-29 (hex) VMware, Inc.
000C29 (base 16) VMware, Inc.
3145 Porter Dr.
Palo Alto CA 94304
UNITED STATES

The second standard VmWare code with starting MAC address **00-0C-29-xx-xx-xx**

Third Set Of Address:

00-50-56 (hex) VMWare, Inc.
005056 (base 16) VMWare, Inc.
44 ENCINA AVENUE
PALO ALTO CA 94301
UNITED STATES

The third standard VmWare code with starting MAC address **00-50-56-xx-xx-xx**.
So at this point we have undertaken all vmware codes.

The VmWare MAC Address Range starts from this three defined Addresses as:

0x01) Mac[A] -----> 00-05-69-xx-xx-xx
0x02) Mac[B] -----> 00-0c-29-xx-xx-xx
0x03) Mac[C] -----> 00-50-56-xx-xx-xx

This is static technique but best way to detect vmware remotely.

Now We will Check The Ethereal Response:

1	0.000000	10.1.1.2	Broadcast	ARP	who has 10.1.1.1?	T
2	0.027588	10.1.1.1	10.1.1.2	ARP	10.1.1.1 is at 00:0c	
3	0.027620	10.1.1.2	10.1.1.1	TCP	1221 > 0 [ACK]	Seq=0
4	0.027982	10.1.1.1	10.1.1.2	TCP	0 > 1221 [RST]	Seq=0
5	0.999540	10.1.1.2	10.1.1.1	TCP	1222 > 0 [ACK]	Seq=0
6	1.003667	10.1.1.1	10.1.1.2	TCP	0 > 1222 [RST]	Seq=0
7	1.999423	10.1.1.2	10.1.1.1	TCP	1223 > 0 [ACK]	Seq=0
8	2.000327	10.1.1.1	10.1.1.2	TCP	0 > 1223 [RST]	Seq=0
9	2.999295	10.1.1.2	10.1.1.1	TCP	1224 > 0 [ACK]	Seq=0
10	3.000306	10.1.1.1	10.1.1.2	TCP	0 > 1224 [RST]	Seq=0

Query is being sent to the system

- ▽ Frame 2 (60 bytes on wire, 60 bytes captured)
 - Arrival Time: Jun 2, 2006 21:14:36.668357000
 - Time delta from previous packet: 0.027588000 seconds
 - Time since reference or first frame: 0.027588000 seconds
 - Frame Number: 2
 - Packet Length: 60 bytes
 - Capture Length: 60 bytes
- ▽ Ethernet II, Src: 00:0c:29:e5:fd:7b, Dst: 00:50:56:c0:00:01
 - Destination: 00:50:56:c0:00:01 (10.1.1.2)
 - Source: 00:0c:29:e5:fd:7b (10.1.1.1)
 - Type: ARP (0x0806)
 - Trailer: 808601100001000000000000020464845...
- ▽ Address Resolution Protocol (reply)
 - Hardware type: Ethernet (0x0001)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (0x0002)
 - Sender MAC address: 00:0c:29:e5:fd:7b (10.1.1.1)
 - Sender IP address: 10.1.1.1 (10.1.1.1)
 - Target MAC address: 00:50:56:c0:00:01 (10.1.1.2)
 - Target IP address: 10.1.1.2 (10.1.1.2)

I think if I am not wrong then we have reached to our supposition and the strategy is being proved.

Thats All done.

Zknk Den

Conclusion:

The strategy whether small or big do take us to the destination.