Ahmed Alkaysi
4/22/17
MIS 5212 Advances Penetration Testing

OS Analysis Executive Summary

In this experiment, I scanned for vulnerabilities and attempted to penetrate a fresh copy of Windows 7 that was provided from a different class. I used NMAP and Nessus to scan for vulnerabilities, and planned to use Metasploit to exploit found vulnerability. Unfortunately, after scanning using both NMAP and Nessus, I was unable to find any vulnerability for the system.

The first step in this experiment was to find a vulnerability for the provided OS using:

-NMAP
-Nessus

NMAP

1. With NMAP I ran a simple scan: 192.168.29.0/24 on the range of IPs within my network.
2. The scan returned only a couple results, the router and my personal desktop.
3. I decided instead of searching for ports open on the network, it would be easier to search for the MAC address, as I already had this information.
4. In the installed targeted machine’s VM, I clicked Network Adapter settings and selecting Properties from VMware, I was able to retrieve the MAC address info from Advanced page.
5. I than ran this scan: nmap -sP -n 192.168.29.0/24 looking to pair the MAC address found in step 4 to one of the results.
6. I found this MAC: 00:0C:29:63:25:76, which matched what was in VMware, associated with IP 192.168.29.116.
7. I then ran a simple NMAP scan on the IP, it gave a message that the Host seemed down.
8. As a last resort, I used nmap -Pn 192.168.29.116, in case the pings were being blocked, and received message saying all 1000 ports were filtered.
9. With no luck finding any open ports, I decided to move on to Nessus.

Nessus

1. I created a Basic Network Scan and entered the IP Address 192.168.29.116.
2. Nessus began scanning the system, taking roughly 15 minutes to complete.
3. After it was complete, there were no vulnerabilities found, only ‘4’ Info.
4. Looking at the info, I thought it was interesting one of the results were determining the MAC address belonging to VMware.

Failing to discover a vulnerability after using NMAP or Nessus leaves me to believe that there were no services running on any of the ports. It looks like this fresh install of Windows 7 had been patched to the latest update and any services that might have been running have been disabled. The team that built this OS did a good job not leaving any initial security gaps.