COMP 4108 – COMPUTER SYSTEMS SECURITY

Experience 5 – Penetration Testing

Student Name: Ben Cendana
Student #: 100811212
Date: February 12 2018

Table of Contents

1.0: Introduction

One of the newest and exciting subfields to grow from Cybersecurity is Penetration Testing or ethical hacking. The idea behind penetration testing is in order to determine how to best protect a system many simulated attacks are launched to test against the systems potential weaknesses. Once these weaknesses are exposed they can be patched.

2.0: Armitage Tool

2.1: Attack Setup

To conduct the penetration testing we will use a tool called Armitage, once we have started Armitage we will need to scan the network we want to launch a simulate attack on.

To do this we click on *Hosts -> Intense Scan*

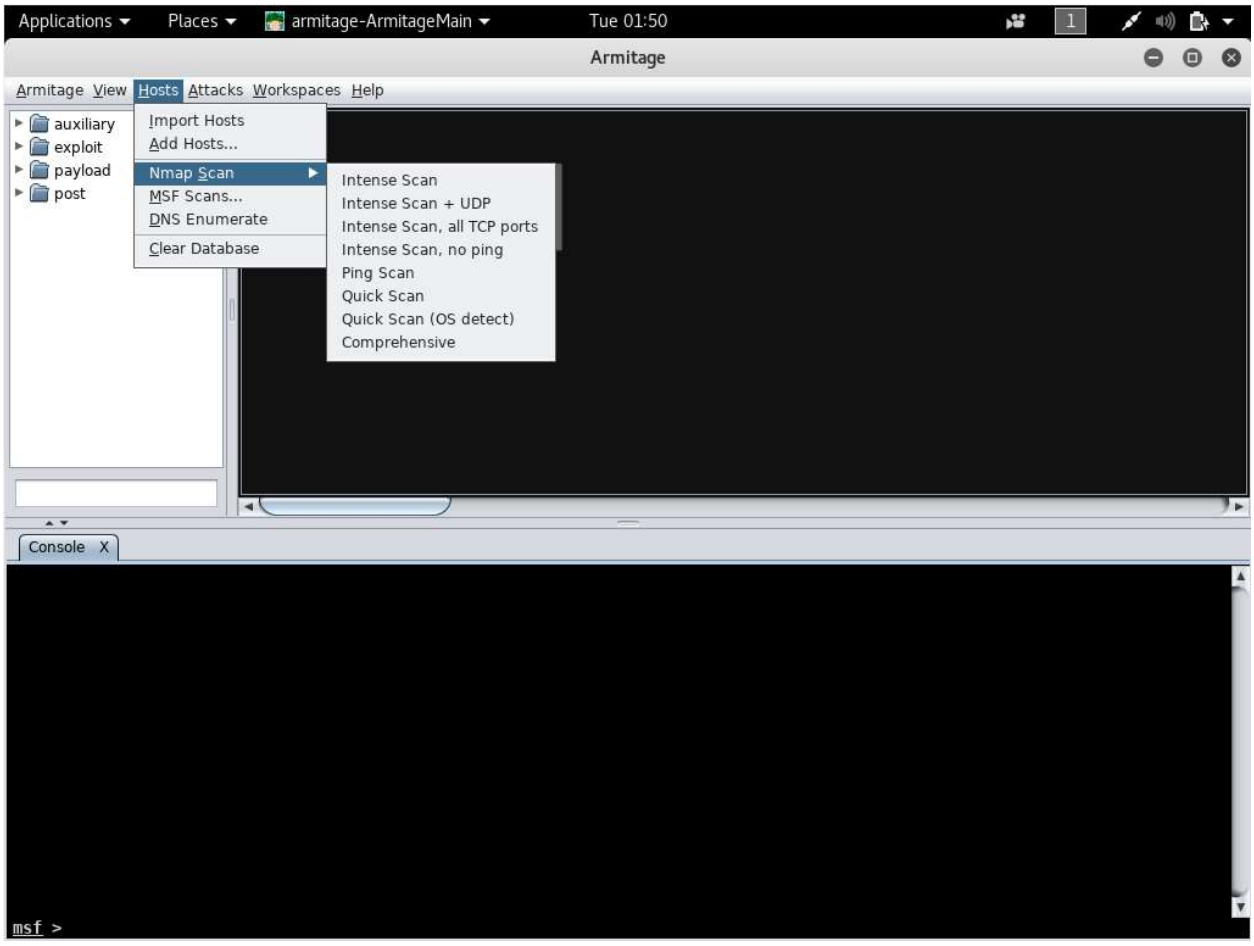

Figure 1: Starting A Scan With The Armitage Tool

The next step is to enter the default gateway IP on the network we want to simulate an attack on, in this example we are using 192.168.2.60/24.

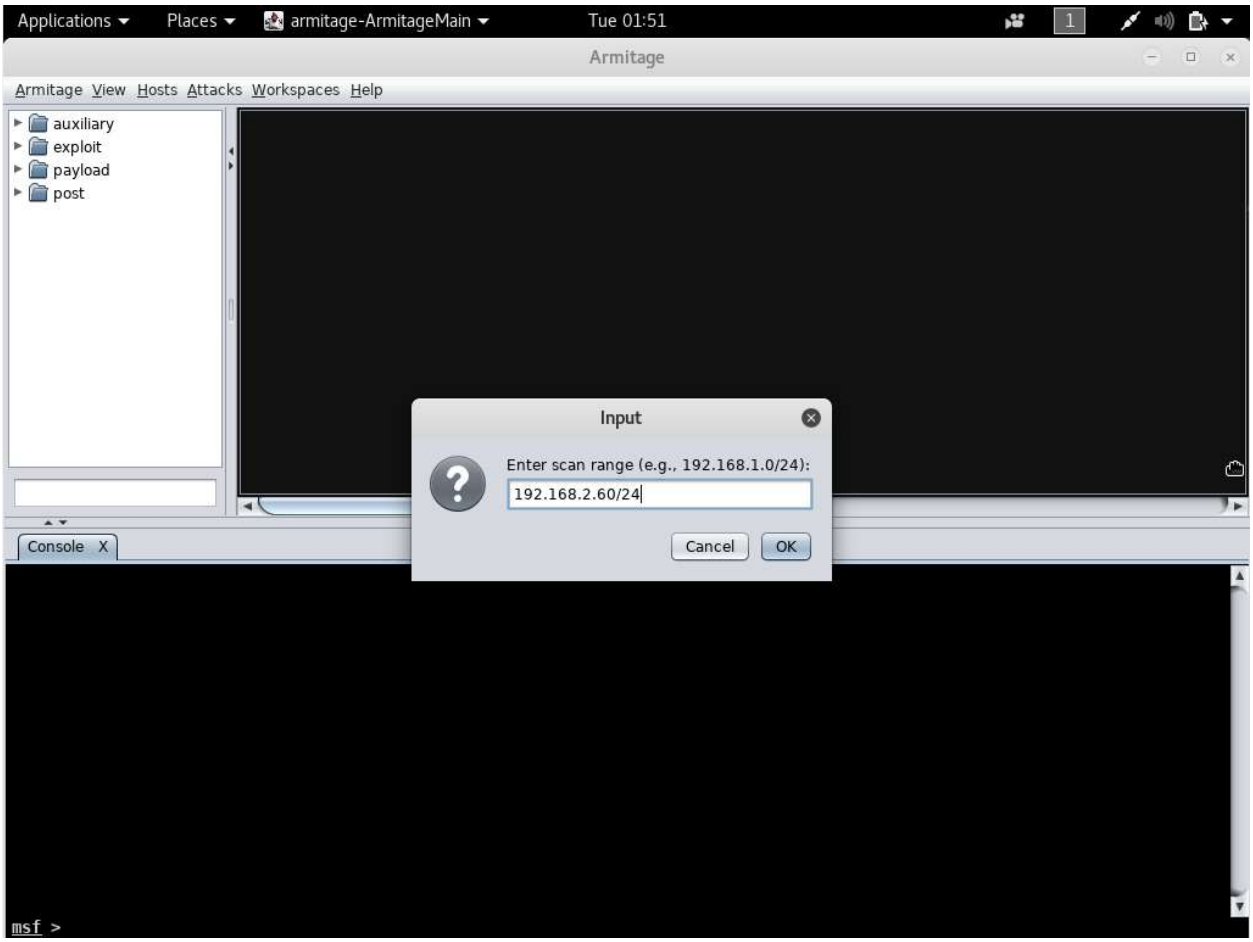

Figure 2: Entering The Default Gateway IP.

Once the IP for the Armitage tool is entered the tool will start Scanning for hosts (Figure 3), note it may take upwards of 30 minutes depending on the network topology.

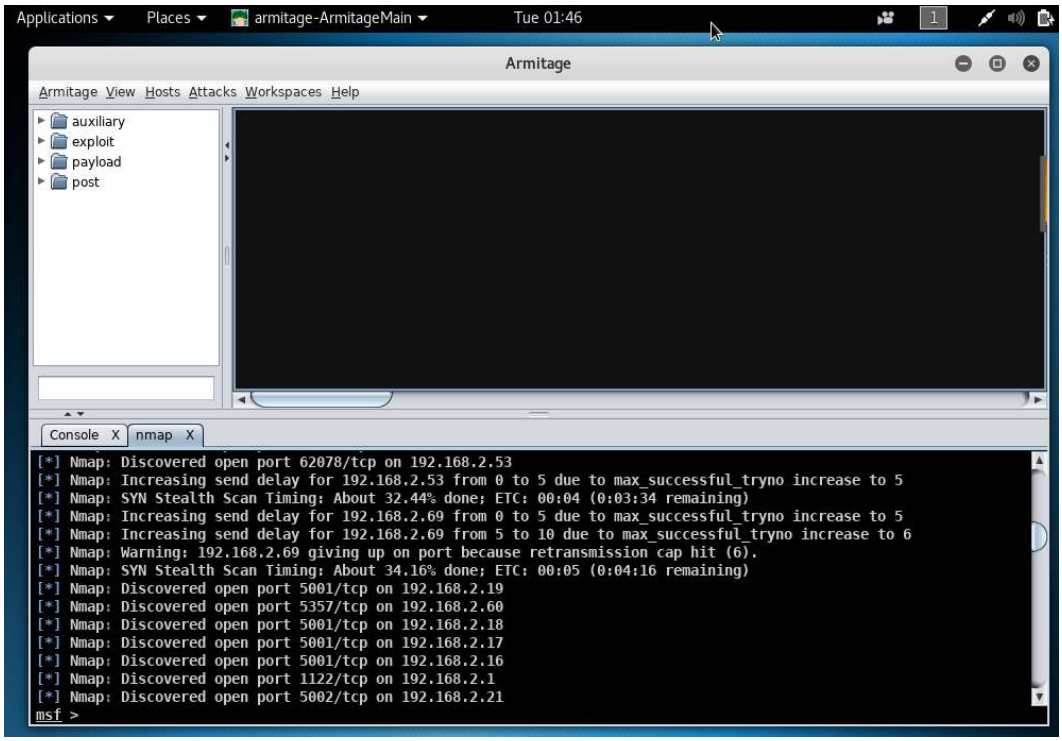

Figure 3: Scanning For Hosts.

After the scan has been completed we will be shown a list of available hosts on the network.

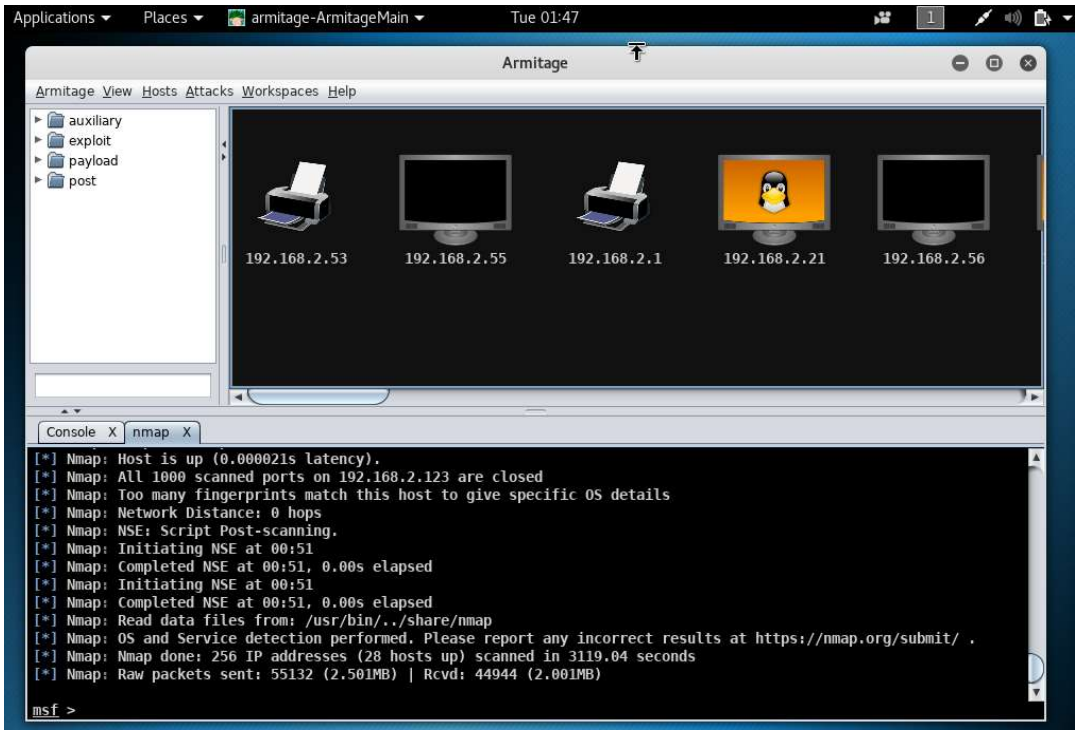

Figure 4: Scanning For Hosts.

We can then click on any of the icons, each represent a hosts on the network and we can simulate an attack

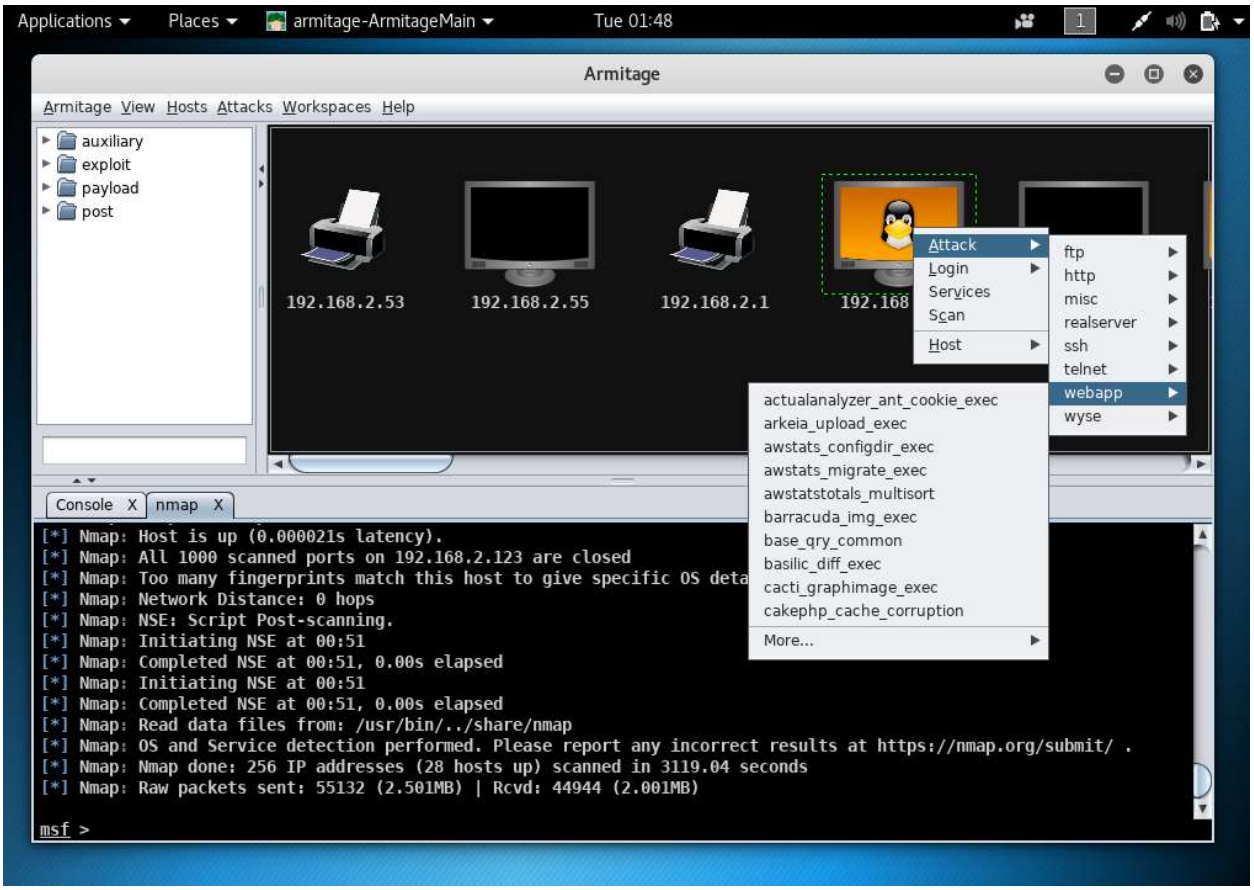

Figure 5: Launching A Simulated Attack.

3.0: Launching Attacks

3.1: Samba Attack

For this experiment we choose the samba vulnerability which is a vulnerability that lead to the WannaCry Randsomware virus.

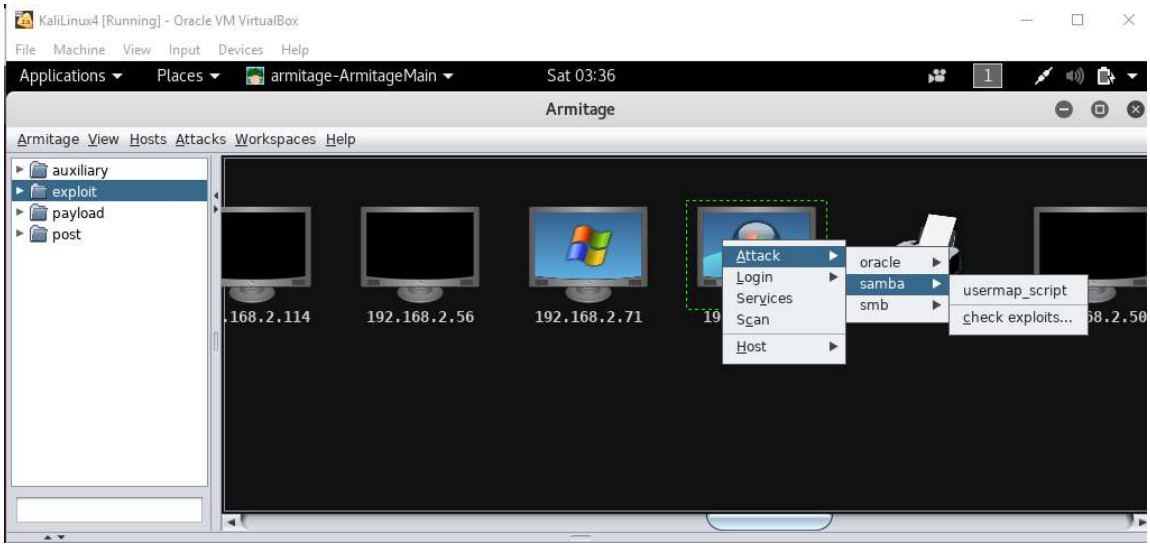

Figure 6: Scanning Attacks

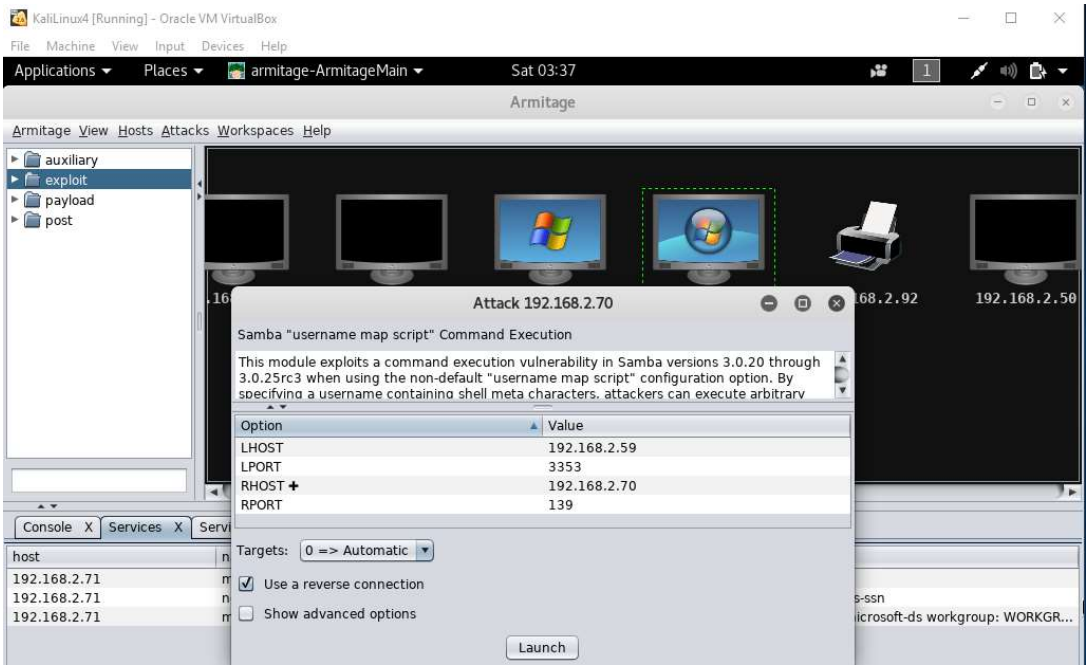

Figure 7: Launching A Samba Attack

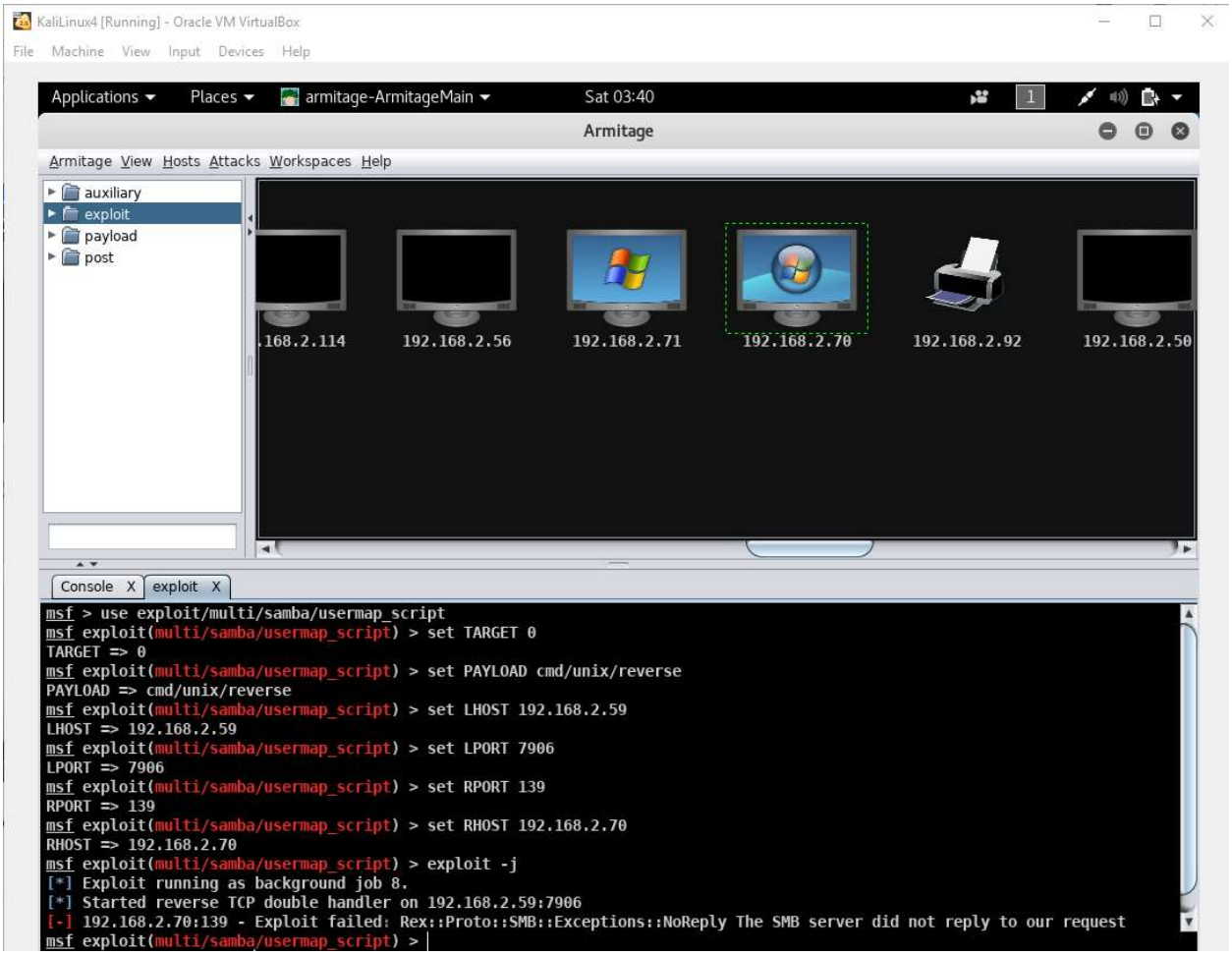

Figure 8: Results Of The Samba Attack

As we can see in Figure 8, the payload and the simulated attack failed meaning the systems defenses are built to protect from the SMB vulnerability.