Course Project: Milestone 1

Cesar Munguia

03/12/2024

—

IS-4543-001

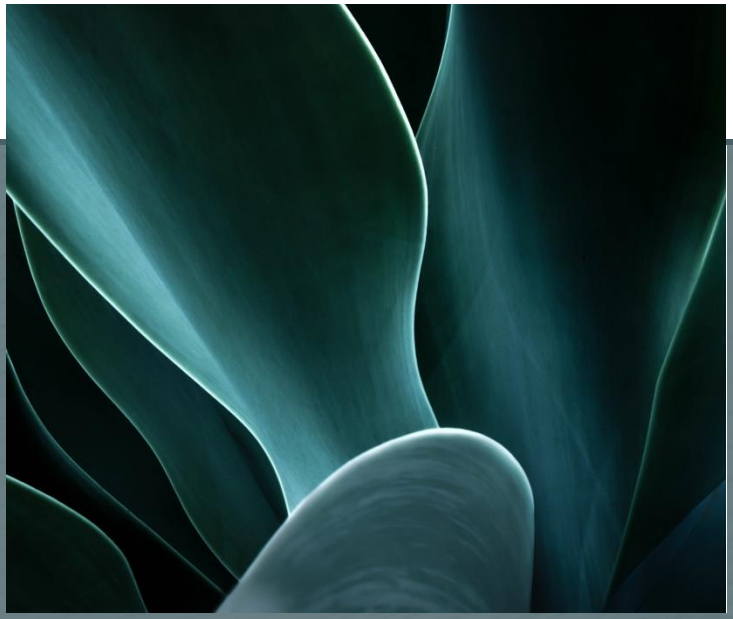
—

Jose Mireles

Objectives

Each milestone submission will be a write-up that includes:

- What did you do?
- What did you learn?
- Documentation of your work
  - Screenshot
  - Picture
  - Video
  - Interpretive Dance



Project Proposal

The project involves in-depth analysis of a virtual machine infected with malware, focusing on understanding the malware's behavior, persistence mechanisms, and potential impact on the system. Through forensic techniques and dynamic analysis, I will dissect the malicious code, identify evasion tactics, and extract indicators of compromise. The project aims to enhance cybersecurity skills by providing hands-on experience in malware analysis and incident response, crucial for defending against and mitigating the effects of sophisticated cyber threats.

- Milestone 1: Create a sandbox to run the malware in a safe manner and choose a type of malware to utilize

In Milestone 1 I will be mainly focusing on creating a safe environment where the malware can be run properly. This will require me to download a virtual machine and executing certain actions in order to maintain other devices in my network safe and to prevent the malware of spreading. This is a crucial step because we don't want other devices or people to be put in a vulnerable spot when running the malicious program.

Summary of Activities

I will need to start off by getting a virtual machine that is going to play the role of the victim. In this case, I've decided to use an operating system that can be considered new or up-to-date at the moment, which is a Windows 10 operating system. My goal here is to come very close to a real-world scenario that would possibly occur in a company, or a scenario where an individual downloads something malicious in the internet and infects the computer.

I will be using VMWare as the hypervisor to run my sandbox. Since I've been using the program for quite a while now due to IS classes, there is no need to download it again. Next, the Windows 10 machine is a VM that I've had in the past already, so, there's also no need for installation. Overall, this was just a matter of configuring the virtual machine. This is actually a VM I've used to conduct malware analysis. It includes several tools like sysinternals from Microsoft.

I started by powering up the virtual machine (refer to screenshot 1). Then, I went to settings to change the configuration of its network. It was set to NAT, but I changed to host-only (refer to screenshot 2). Then, I changed the IP address manually to 192.168.10.2 (refer to screenshot 3). Then, I opened the command prompt and tried a couple of commands to confirm that the machine is unable to access the external network (internet). I tried command **ping www.google.com** and **ping 8.8.8.8** (refer to screenshot 4). I was able to confirm that the machine couldn't reach the internet. Then, I turned off the proxy of the virtual machine (refer to screenshot 5). Then, I disabled the firewall, more specifically, the domain profile, the private profile, and public profile (refer to screenshot 6). Then, I disabled the Windows Defender by typing "edit group policy" in the search bar and disable it from there. More specifically, I went to Computer Configuration > Administrative Template > Windows Components > Windows Defender (refer to screenshot 7). Finally, the most important step was to take a snapshot of the current state of the VM (refer to screenshot 8).

Now, it was time to make a decision on the type of malware I was going to infect the computer with. There are several types of malwares like RATs, spyware, keyloggers, worms, viruses, ransomware and many more. I've decided to choose a spyware/keylogger because coming back to the assumption that an individual accidently clicked on a link inside a spear-phishing email, an attacker might've chosen this particular person to steal sensitive data. This can include either personal information or even intellectual property. I was able to get a sample of the malware in the MalwareBazaar website (https://bazaar.abuse.ch/). The SHA-256 hash is

c3d211758a1061afe67cfeb1e63a4c3cc870534e8b6bab2fbb5423e56268ff96 and the MD5 hash is 7ce0d79c8af824483f1b9fd6f30e456f (refer to screenshot 9).

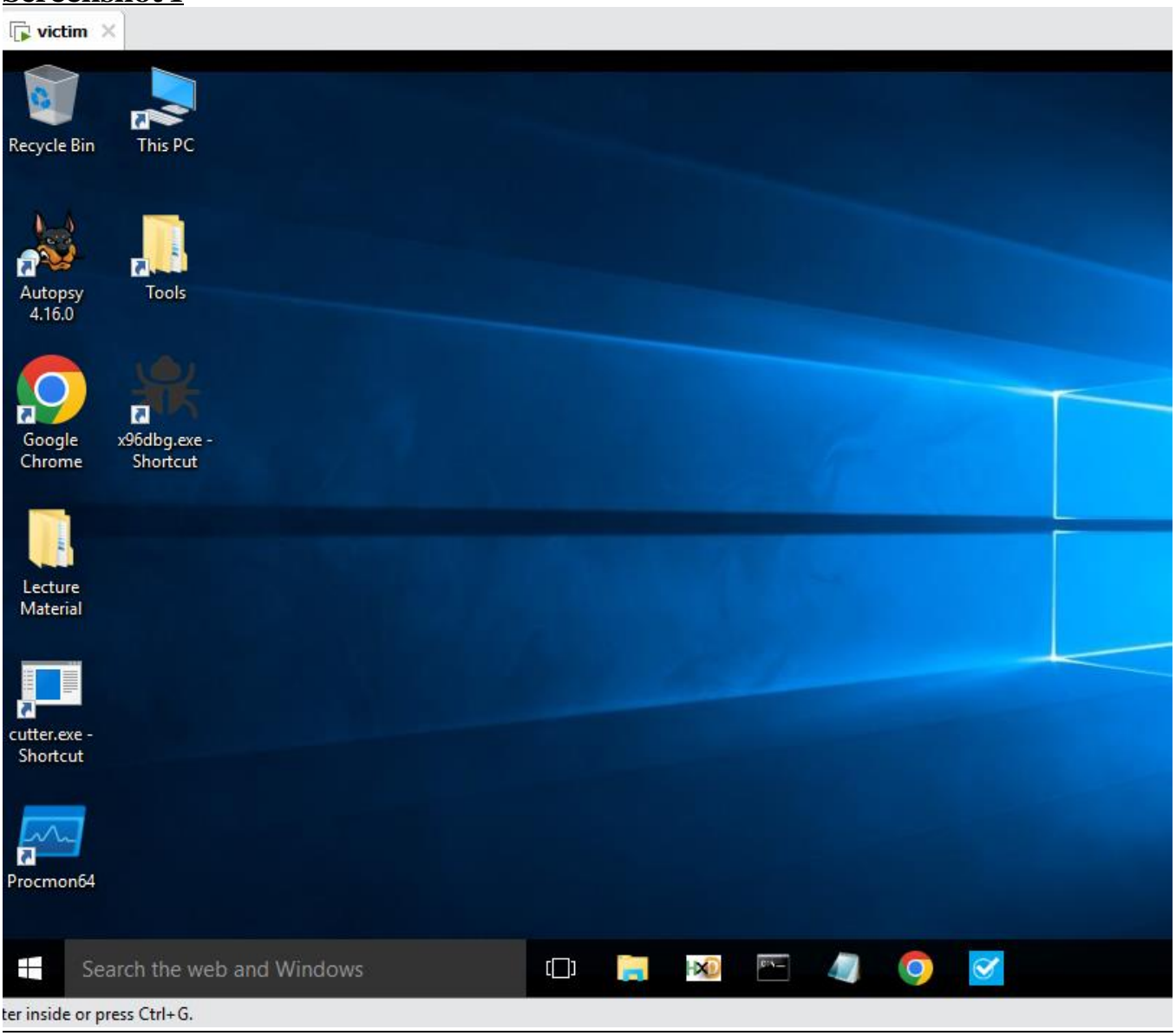
Description of Learning Completed

Creating a separate sandbox area, as carefully explained in your detailed steps, is really important for examining malware and dealing with security issues properly. Using a virtual machine (VM) with a modern Windows 10 system helps mimic real-life situations where people might accidentally interact with harmful software. VMWare, the software managing the VM, ensures it's strong and adaptable. Adjusting the network settings to connect only to the host system and assigning a specific IP address keeps the VM isolated from outside networks, preventing any bad stuff from spreading. By turning off things like proxies, firewalls, and Windows Defender, the environment allows malware to run without interruptions, making it easier to study its actions. Taking a snapshot of the VM's initial state is crucial as it provides a clean starting point for comparison after running the malware. This careful setup not only gives a safe place to analyze malware but also protects the main computer and network from potential harm. In simple terms, the sandbox acts like a controlled area where you can safely study dangerous things without risking damage to anything else. This methodical approach helps researchers understand emerging threats better and strengthens defenses against them, making the digital world safer for everyone.

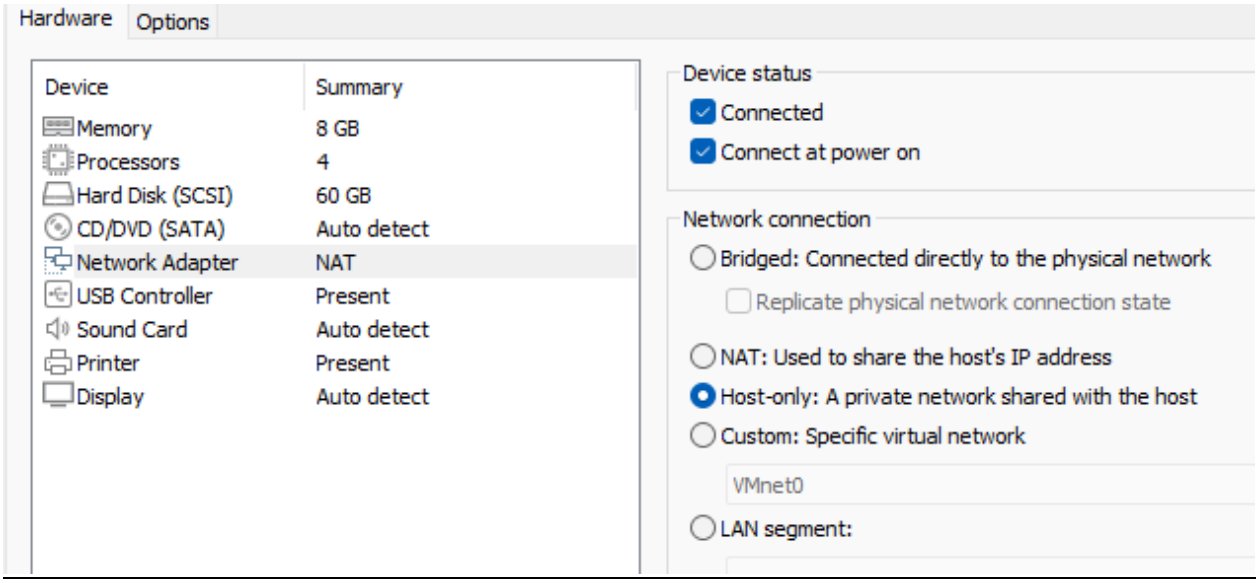
The decision to opt for spyware/keylogger malware indicates a strategic approach. I rationalized this choice by aligning it with a plausible real-world scenario, where an unsuspecting user falls victim to a spear-phishing email. By selecting spyware/keylogger, I emphasized the potential consequences of such an attack, highlighting the threat of sensitive data theft. This encompasses both personal information and intellectual property, illustrating the multifaceted nature of cyber threats and their potential impact on individuals and organizations alike.

Documentation of Work Completed

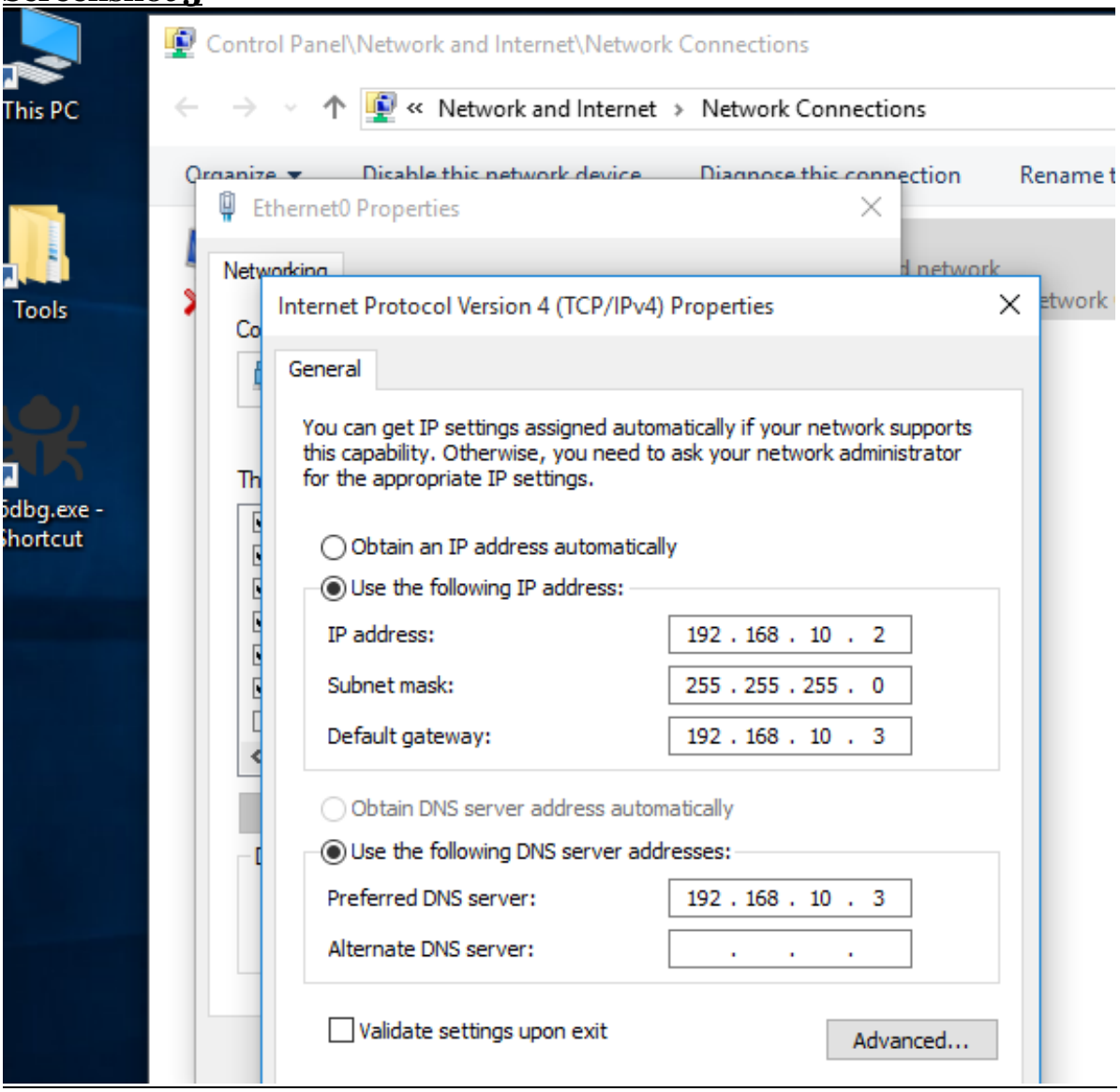
Screenshot 1



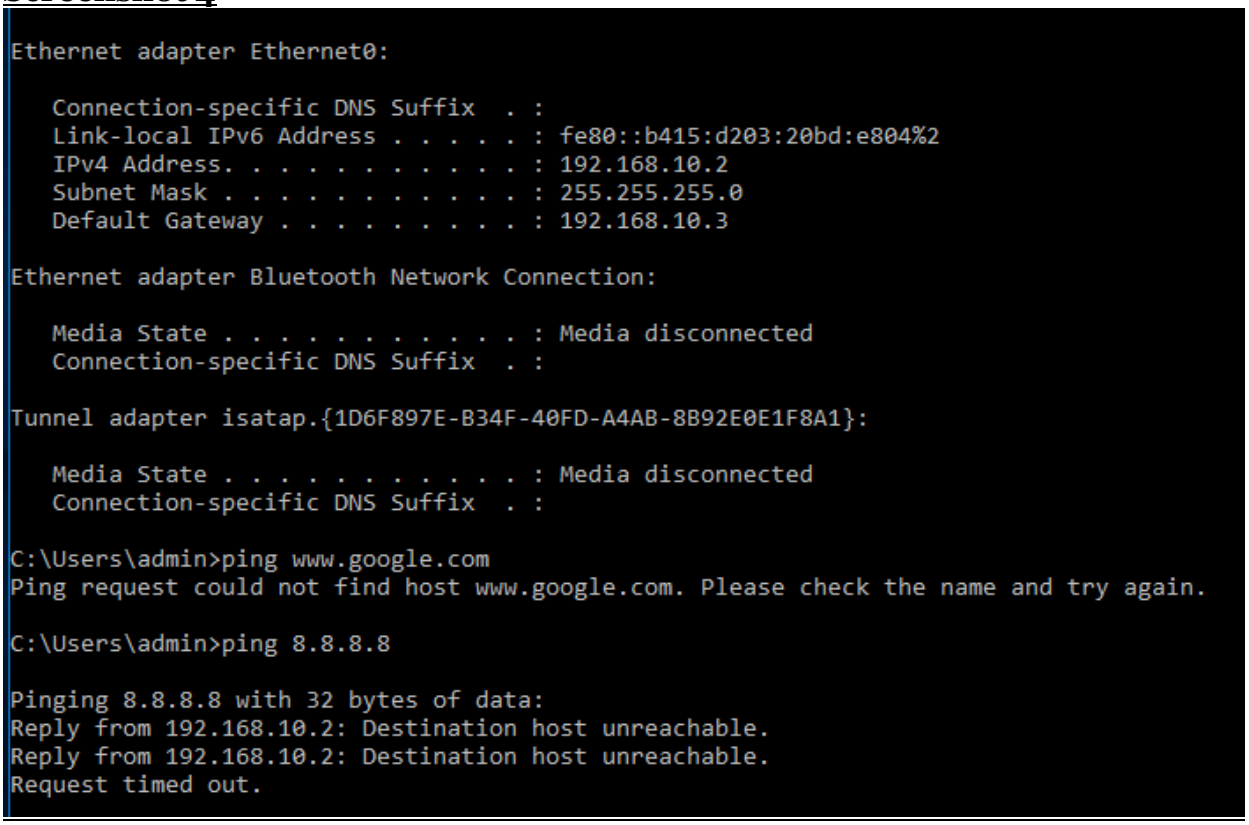
Screenshot 2



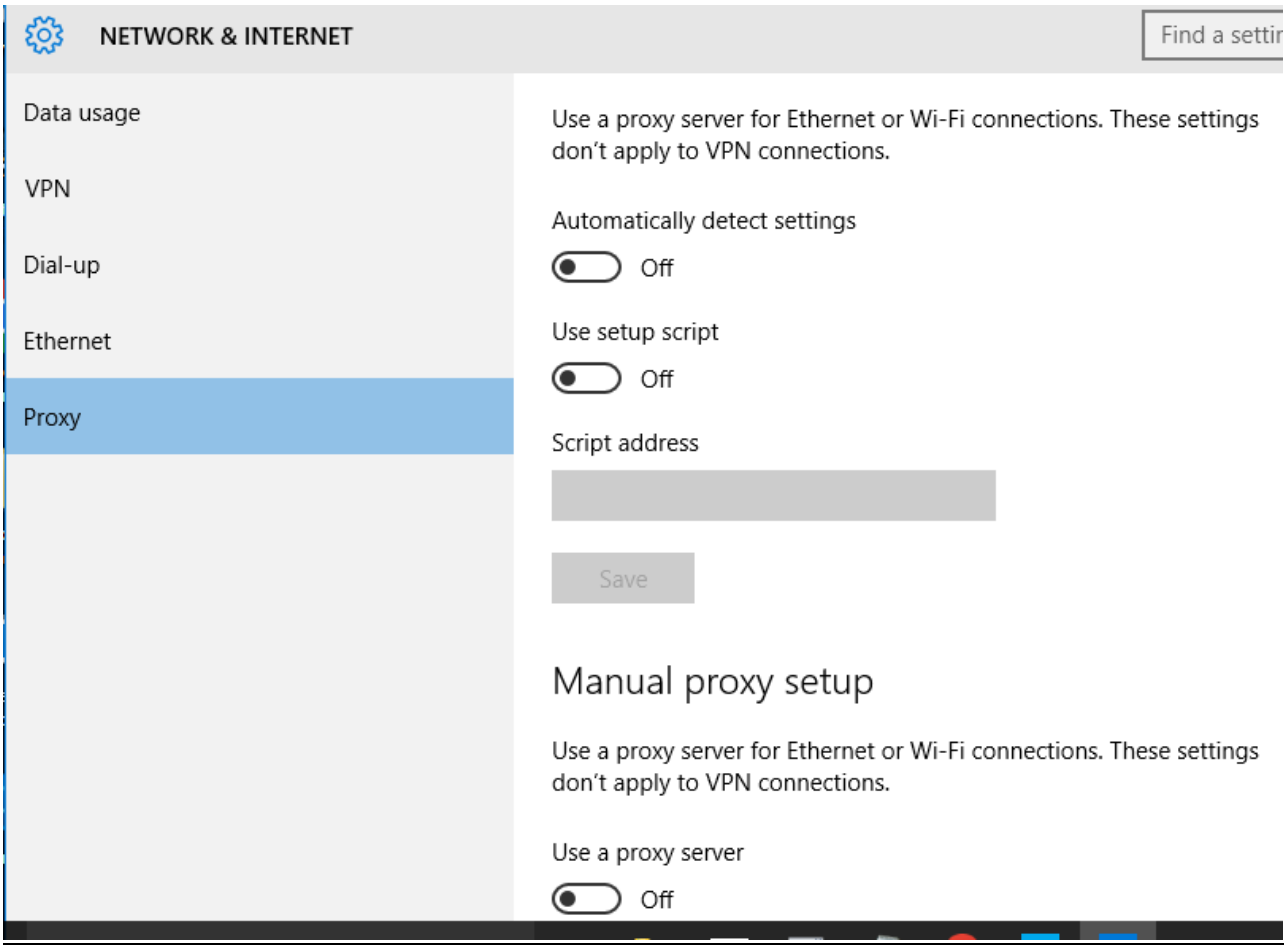
Screenshot 3



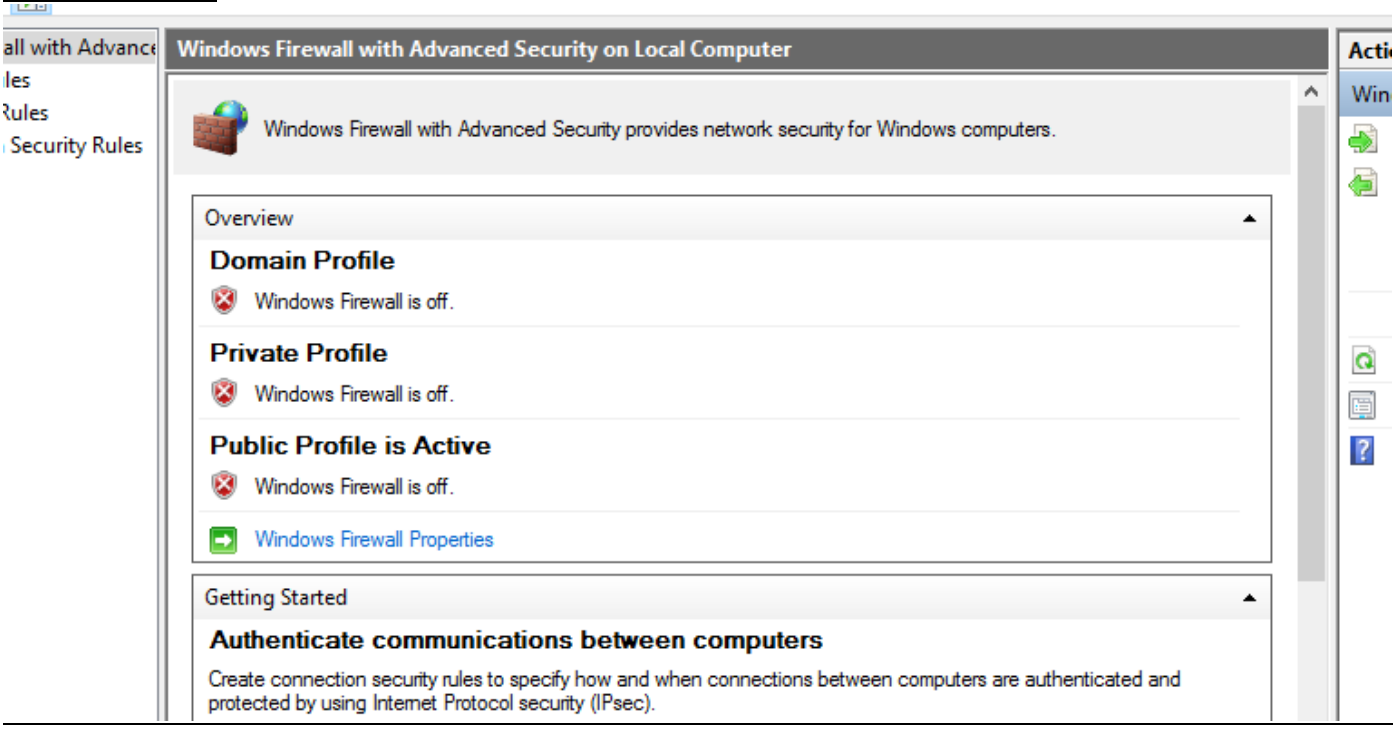
Screenshot 4



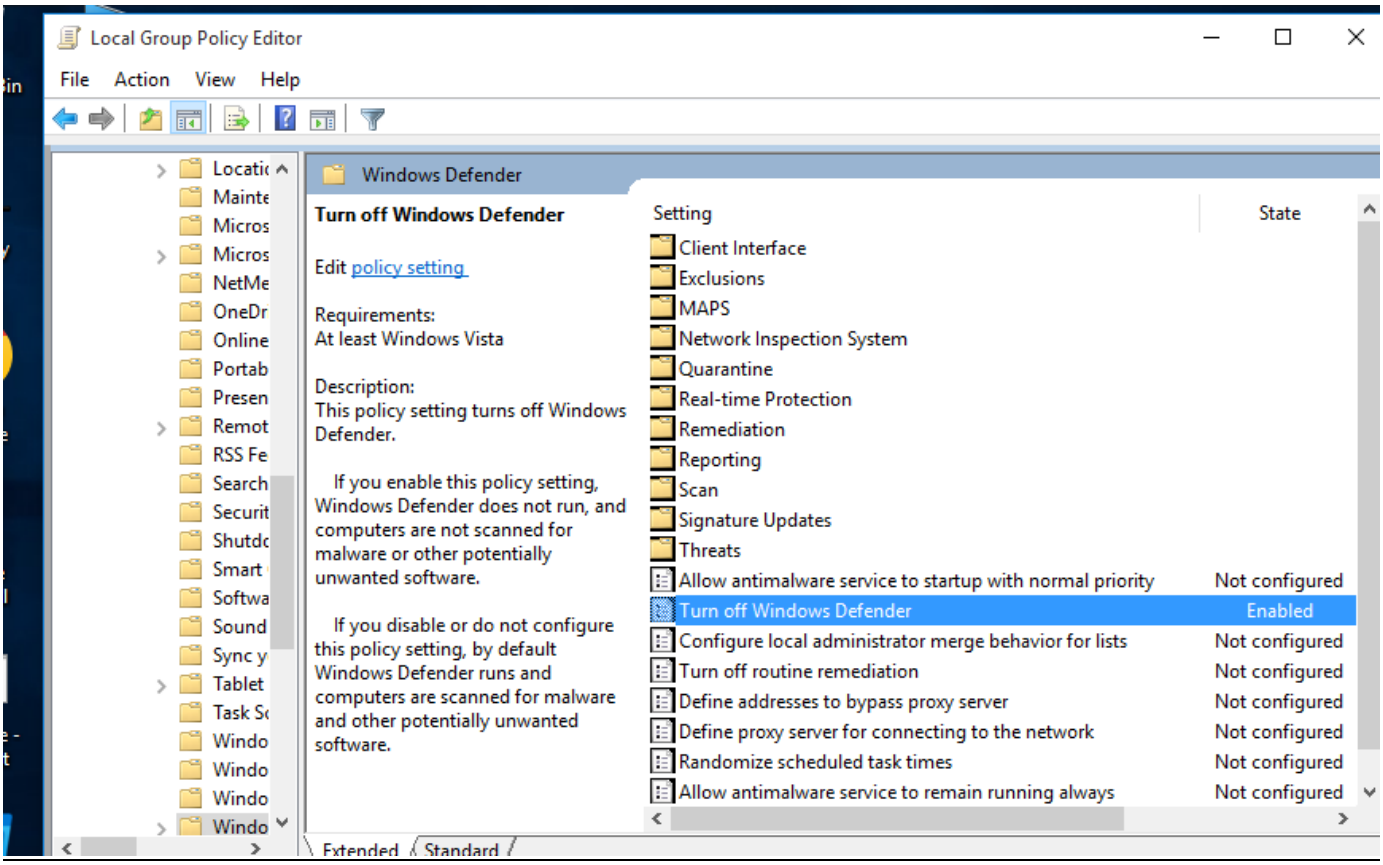
Screenshot 5



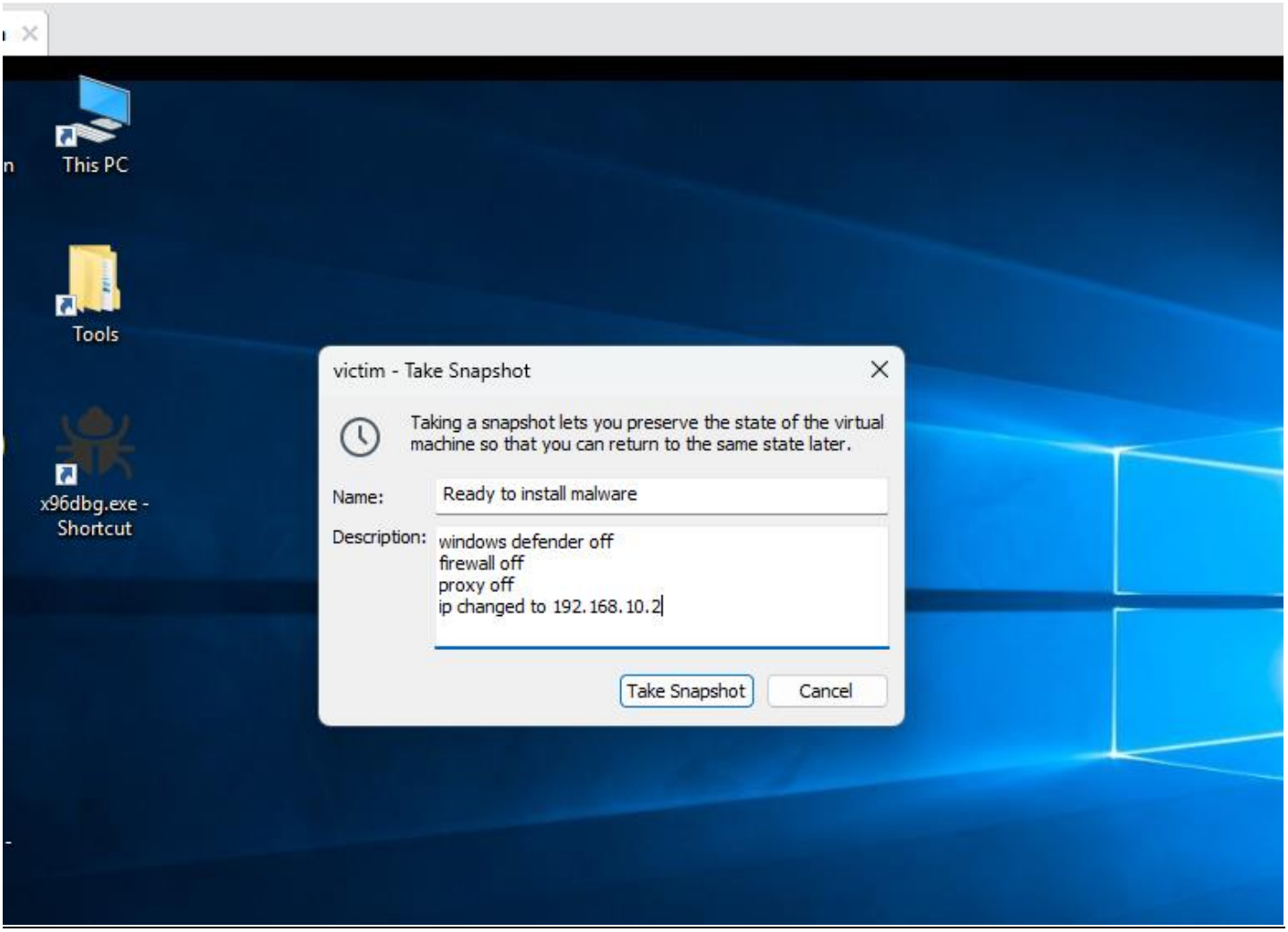
Screenshot 6



Screenshot 7



Screenshot 8



Screenshot 9

MALWARE bazaar by ABUSE.ch — Browse | Upload | Hunting | API | Export | Statistics | FAQ

SHA256 hash:	c3d211758a1061afe67cfeb1e63a4c3cc870534e8b6bab2fbb5423e56268ff96
SHA3-384 hash:	2347074df0fb3d81047ed929d98e82ccb3a313f930cfc71a5c1090cea6798d3eaf457f5c40583934a321b33bcc980654
SHA1 hash:	2292e366de09b5e6e07e3c6863fcc82945c231d1
MD5 hash:	7ce0d79c8af824483f1b9fd6f30e456f
humanhash:	carolina-lima-september-florida
File name:	SystemManager.exe
Download:	download sample
File size:	11'913'469 bytes
First seen:	2022-12-28 07:58:10 UTC
Last seen:	*Never*
File type:	exe
MIME type:	application/x-dosexec