Honeypots Lab

This lab will go over two types of honeypots, Pentbox and Valhala Honeypot. Pentbox will be downloaded and installed on a Kali machine, while Valhala Honeypot will be downloaded and installed on a Windows 10 system.

Before installing any of the honeypots, it’s best to download and install Kali Linux as a virtual machine on a Type 2 Hypervisor using either VMware, Hyper-V, or Virtual Box. Kali can be downloaded from <https://www.kali.org/downloads/>. It is recommended to install the 64-Bit version of Kali and allocate two cores of the processor, 4GB of Ram, and at least 40 GB storage space, but this will come down to the specification of the host system. The second honeypot will run on a Windows 10 system. The Windows 10 OS can be downloaded from the Microsoft website. Allocate at least one core from the processor, 4GB of Ram, and 40 GB storage for the Window 10 VM. Both the Kali and Windows 10 virtual machines should have their network adapters set to “Bridge” connection. The Windows 10 VM should have its firewall disabled which can be done by searching for firewall in the search bar at the bottom left of the home screen.

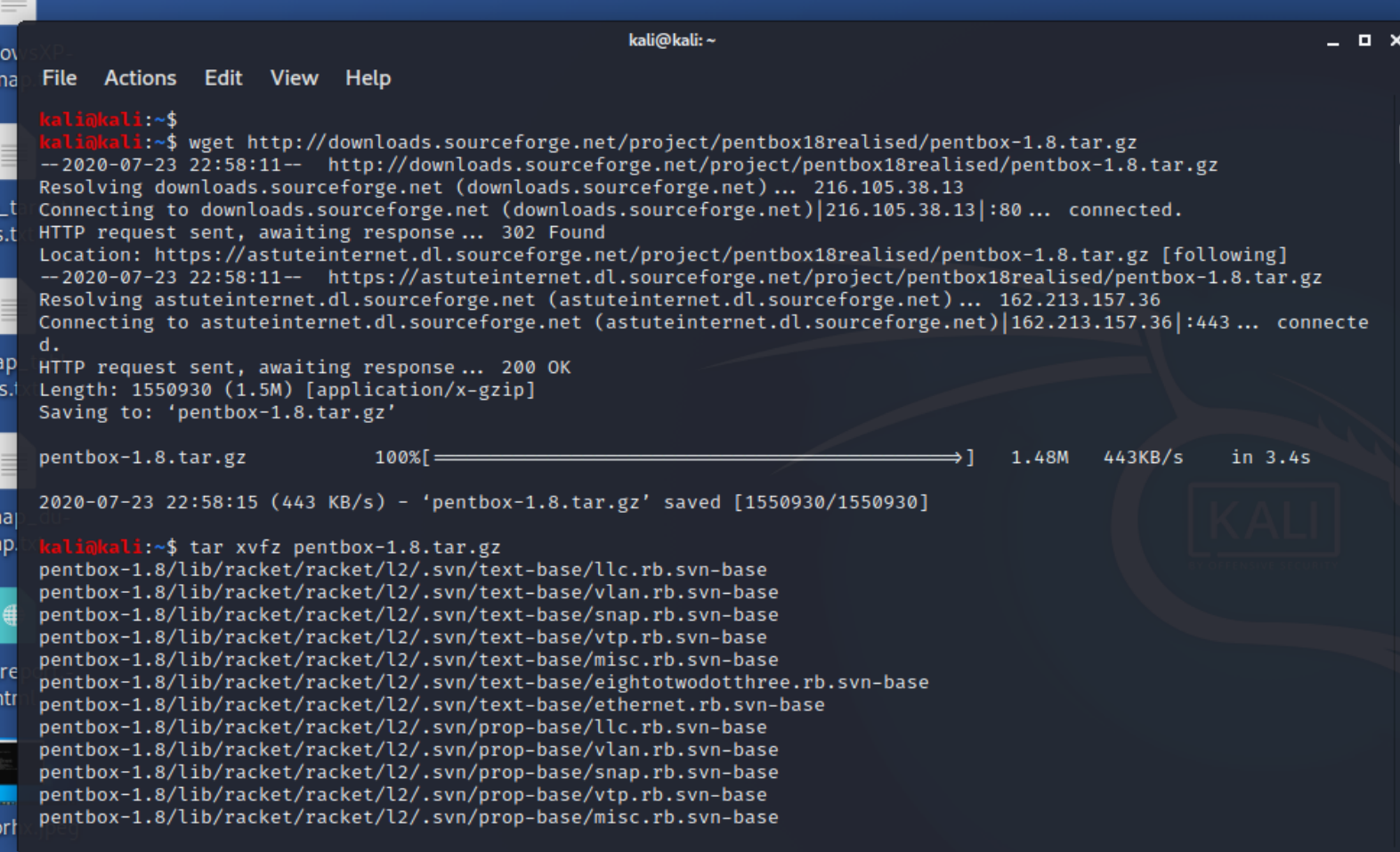
Note down the ip addresses of both virtual machines. On Windows 10, this can be done by selecting the start button at the lower left corner of the screen, type cmd in the search bar, opening command prompt (cmd), and using the **ipconfig** command. For Kali, open the terminal and type **sudo ifconfig**. Lastly, have each VM ping between themselves to see if they can reach each other.

Pentbox:

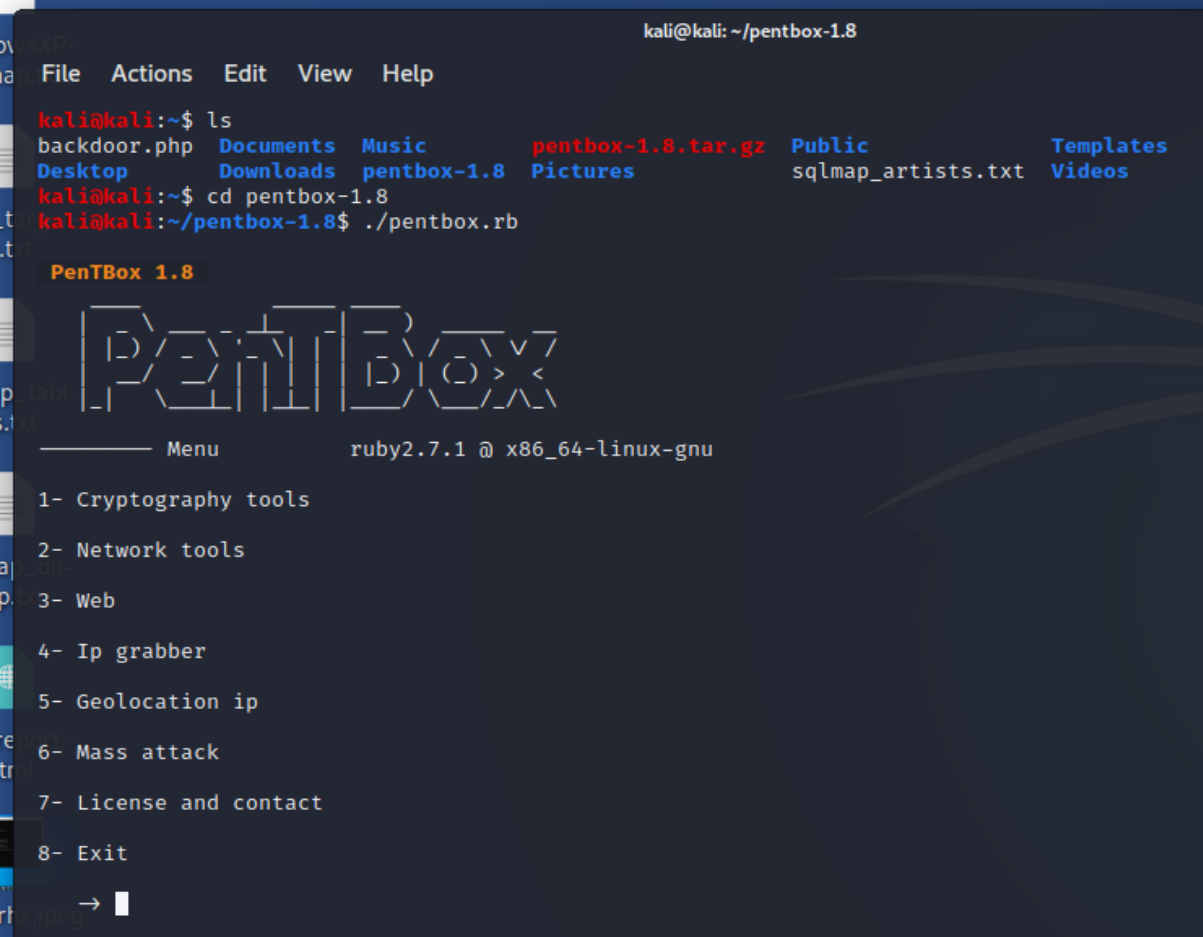
Pentbox is a software used on Linux that contains a suite of tools including a honeypot. To install Pentbox on a Kali system, open the terminal and type the command:

**wget** [**http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz**](http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz).

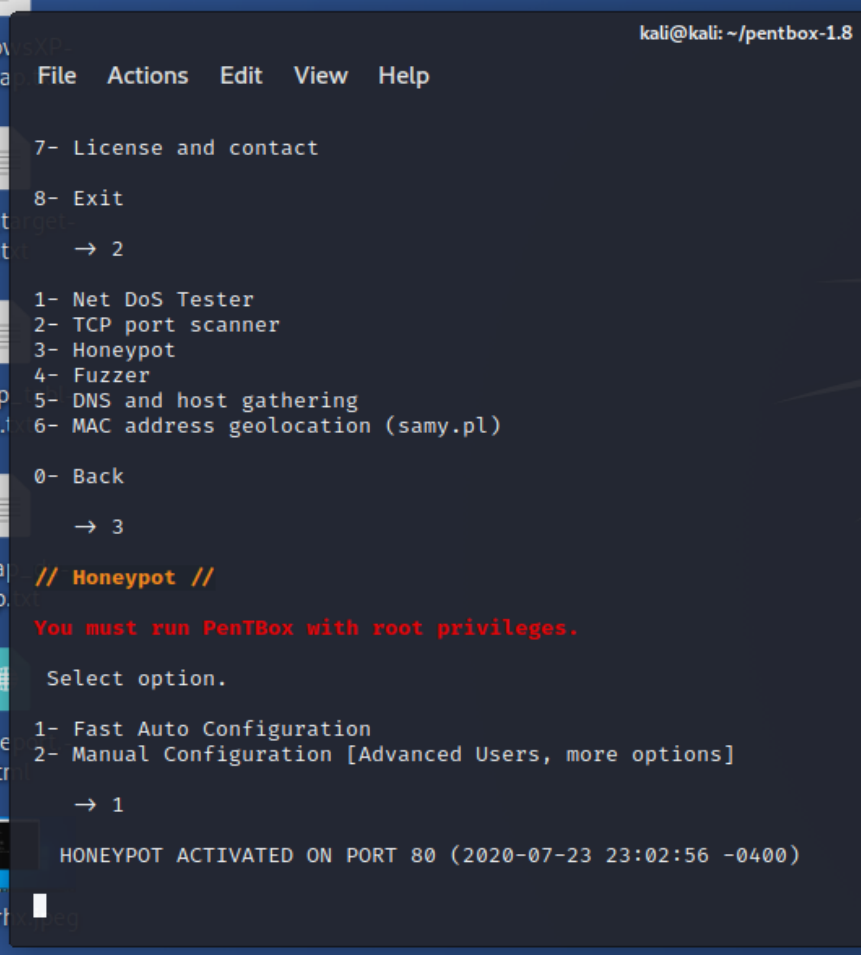
Next, you will need to extract it using the command: **tar xvfz pentbox-1.8.tar.gz**.



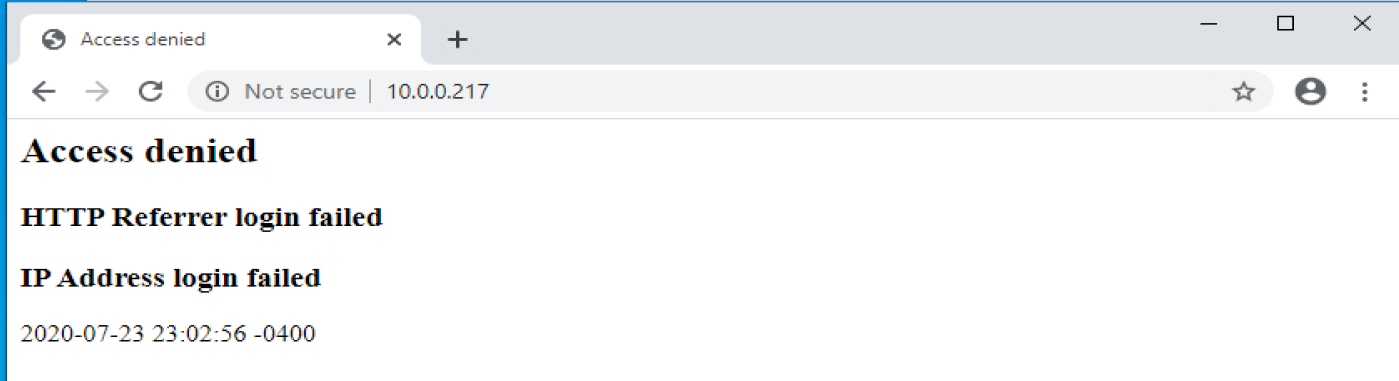
Navigate to the “pentbox-1.8” directory and start Pentbox with **sudo ./pentbox.rb**. Once it opens, you should see the title at the top and a menu listing several tools.



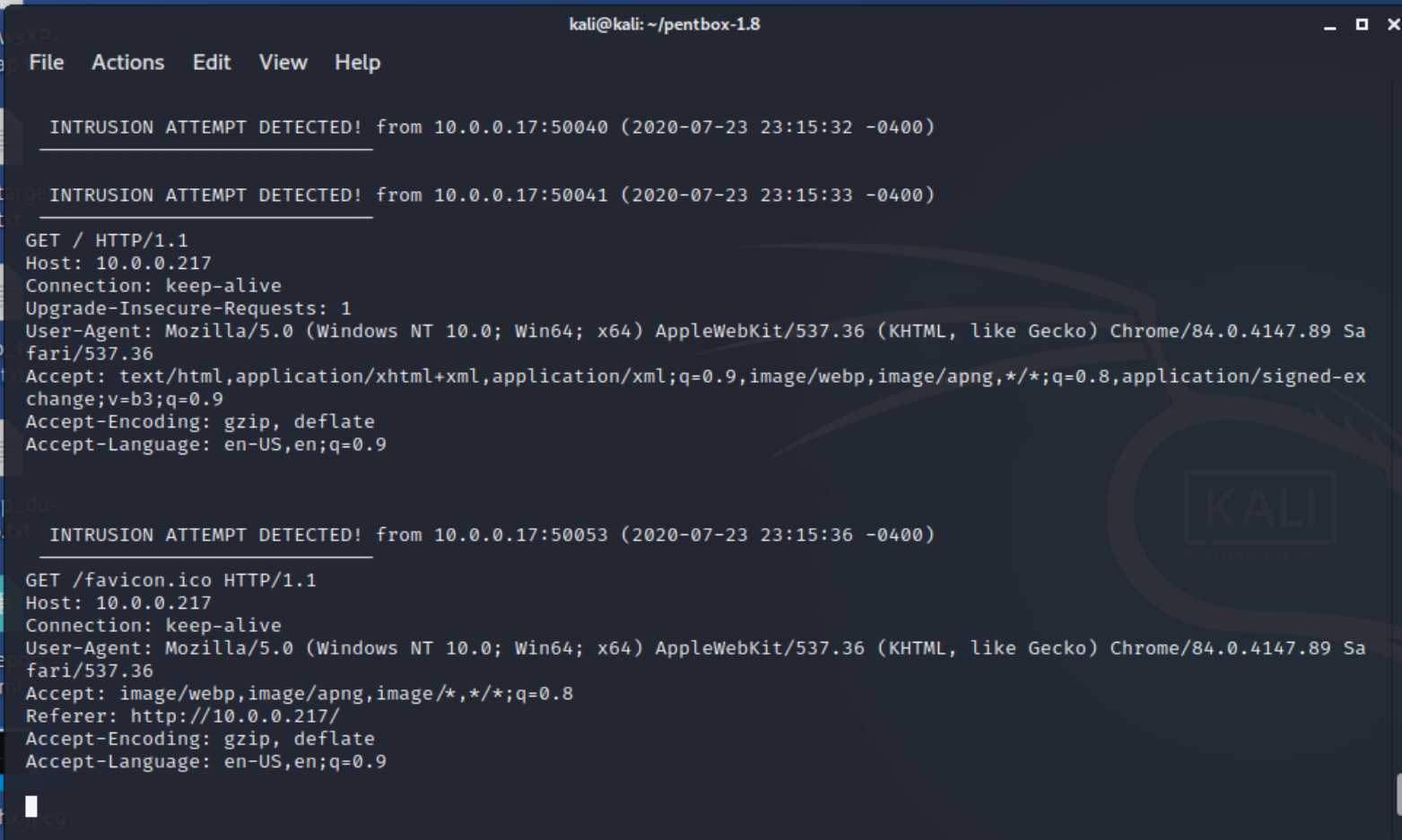
Select 2 for “Network Tools” from the menu and then 3 for “Honeypot.” There will be two options, “Fast Auto Configuration” and “Manual Configuration.” Select 1 to quickly configure the honeypot to listen to port 80.



Move to the Windows 10 VM and open a web browser. In the URL, type in the ip address of your Kali machine to try to connect to it, which will prompt with an access denied message.

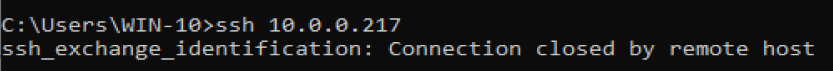


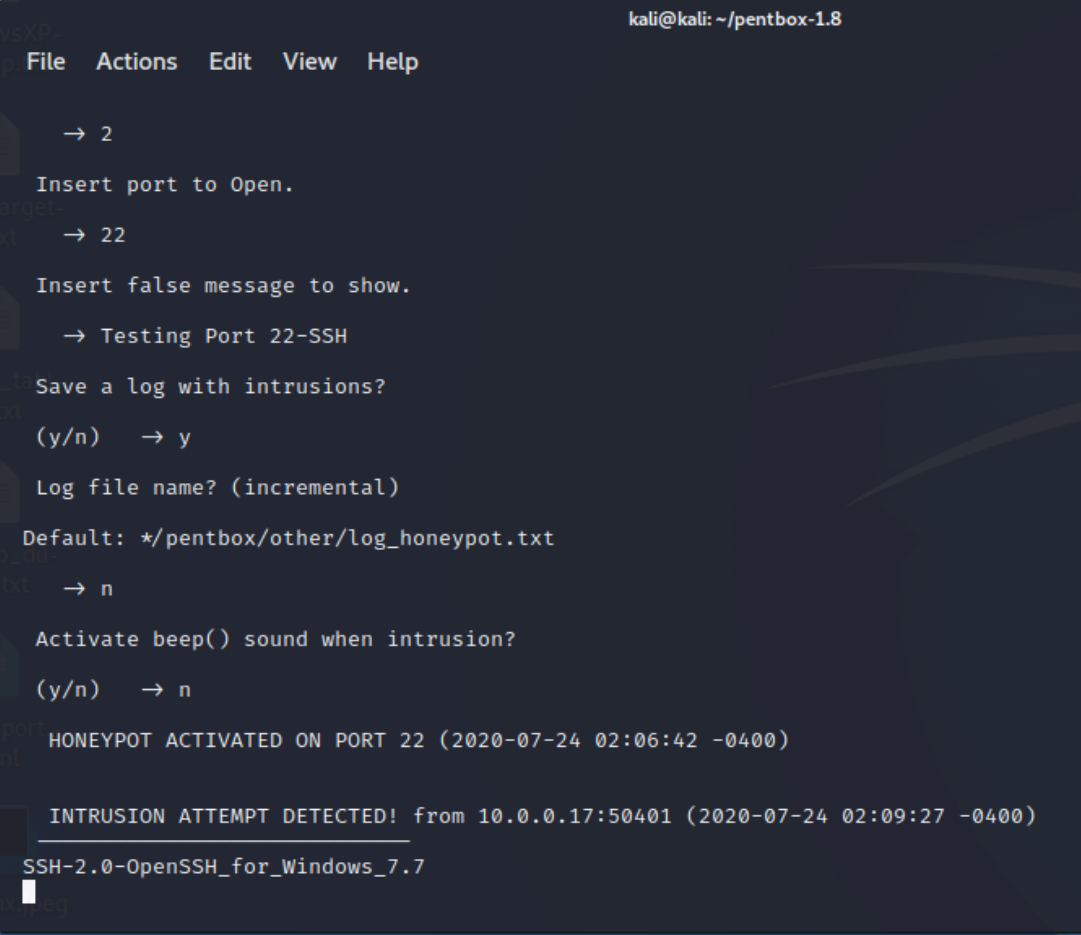
If you go back to Pentbox on your Kali machine, you should see that the honeypot captured that a machine attempted to connect to it via an HTTP connection. It should also show the type of machine it was and it’s ip address.



We can also configure Pentbox to listen to specific ports such as SSH. To do this, relaunch Pentbox, follow the instructions as before, however, when prompted the choice between “Fast Auto Configuration” or “Manual Configuration,” choose option 2 (Manual Configuration). Then type 22 for the “Insert port to Open.” You can type whatever message you want for “Insert false message to show” and then select y (yes) for “Save a log with instructions.” For the following questions, just select n for no. Once the configuration is complete, you will receive a message letting you know that the honeypot is activated and listening for port 22.

Try to connect to Kali from your Windows 10 VM by an SSH connection. This can be done by opening command prompt and typing **ssh** followed by the ip address of the Kali machine. You should receive a message letting you know that the remote host had terminated the connection.

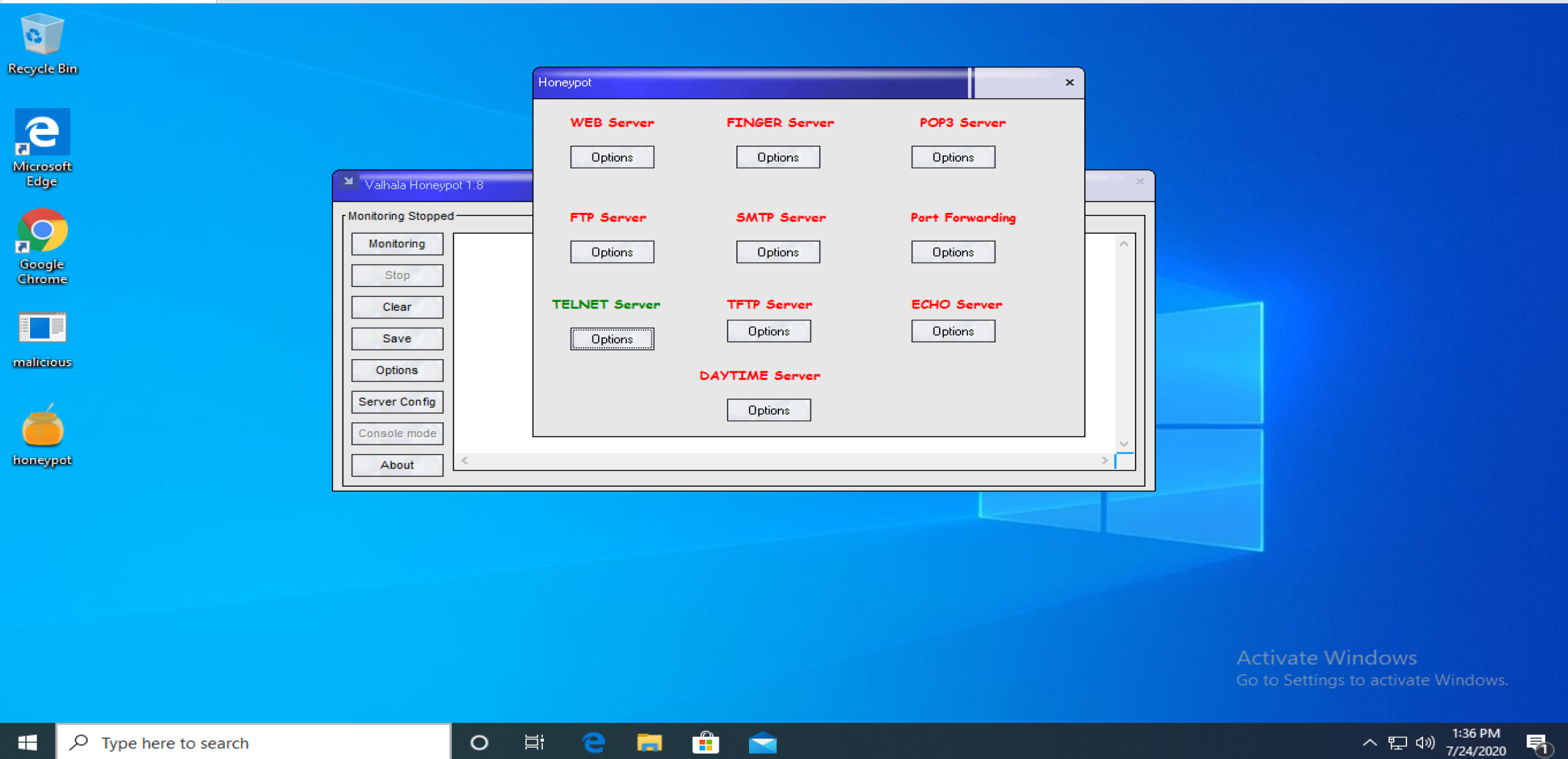




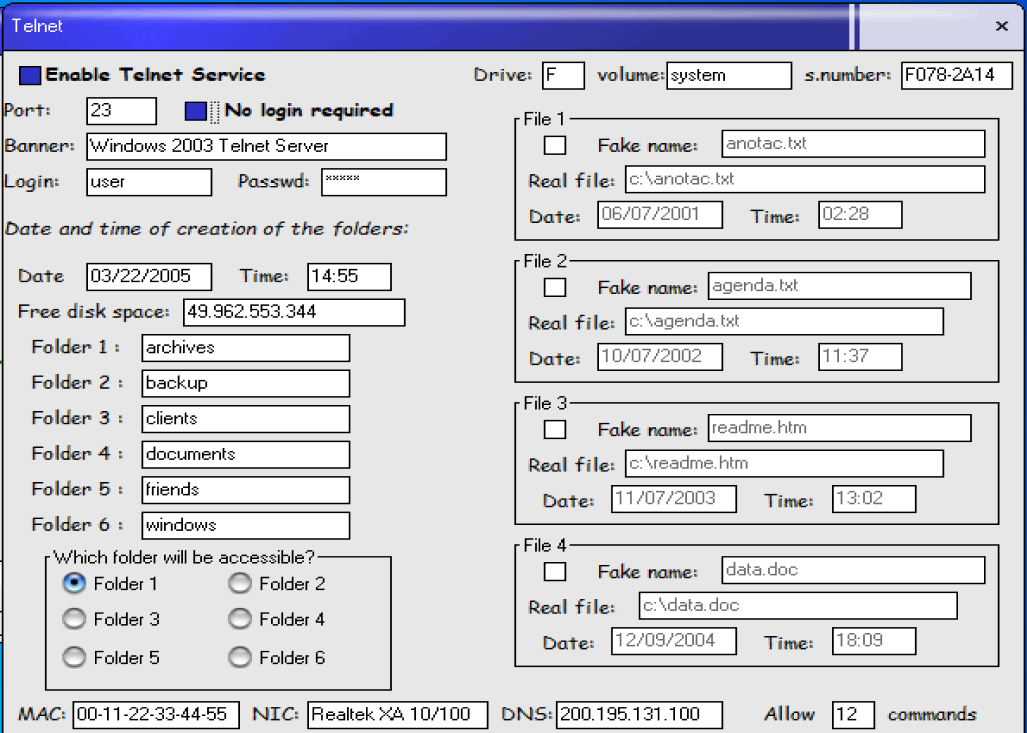
Back at your Kali machine, Pentbox will let you know that an SSH connection was initiated by a Windows system, providing also an ip address and a timestamp.

Valhala Honeypot:

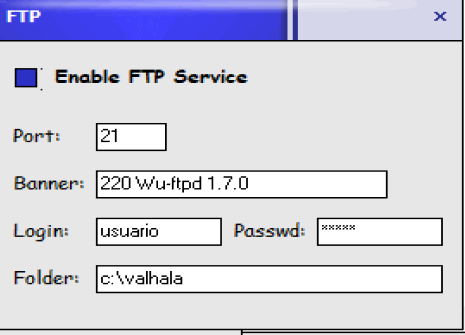
Valhala Honeypot is a honeypot meant to be installed on a Windows system. It is very simple to learn and set up as it provides a GUI format. To download the honeypot on your Windows 10 VM, open a web browser and navigate to the URL <https://sourceforge.net/projects/valhalahoneypot/files/valhalahoneypot/valhala180/valhala180-english.zip/download>. Start Valhala Honeypot by opening the .exe file. After it opens, select “Server Config” to open a second window which will display multiple types of servers. These servers are used to listen on specific network ports for any connections from outside sources.



Select the options button under “TELNET Server.” When the window open, select to “Enable Telnet Service” and “No login required.”

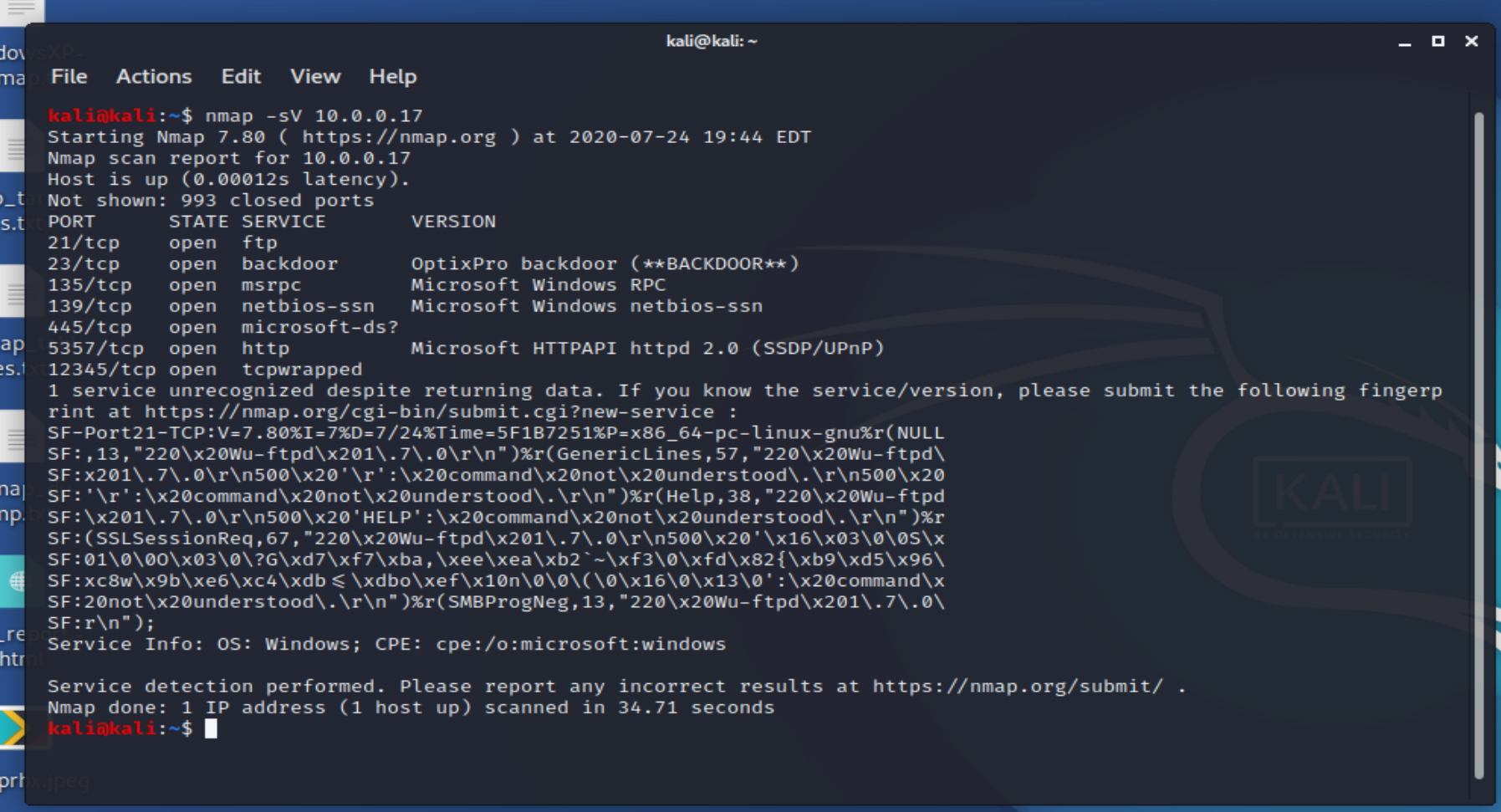


Exit out of that window and select options under “FTP Server” to “Enable FTP Service.” If you get a prompt that says that the “c:\valhala does not exists,” just click OK. Exit out of this window and the “Server Config” window and select the “Monitoring” button.

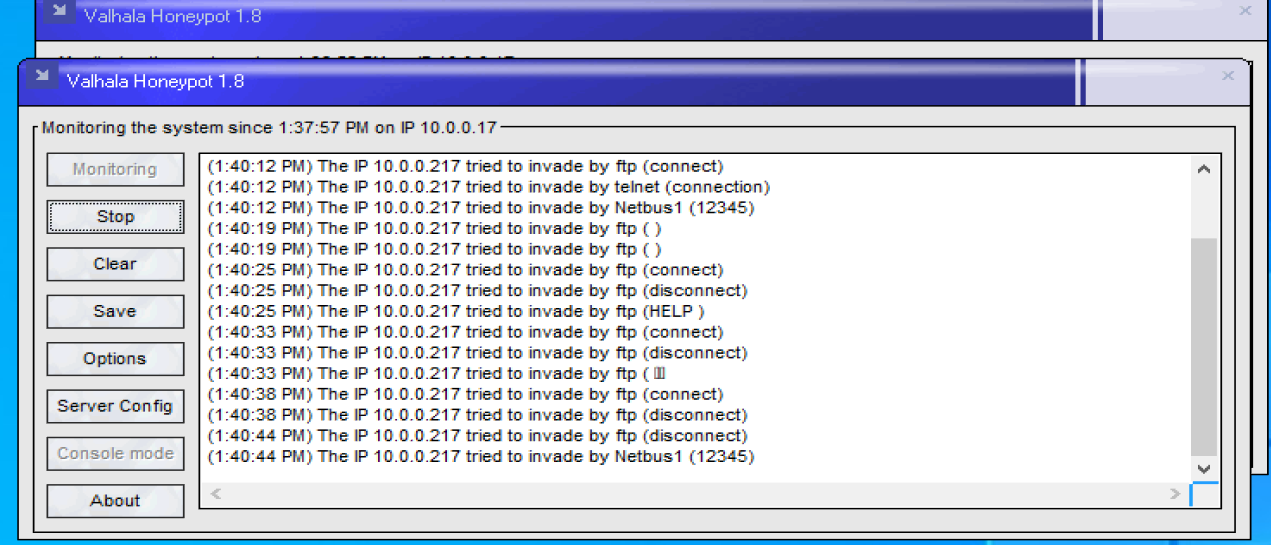


Next, move over to the Kali machine and open the terminal. Scan for open network ports on the Window 10 VM by using Nmap: **nmap -sV (“Windows 10 ip address”)**.

Example: nmap -sV 10.0.0.17



Nmap will detect that the ftp and telnet ports are both open on the Windows 10 VM.

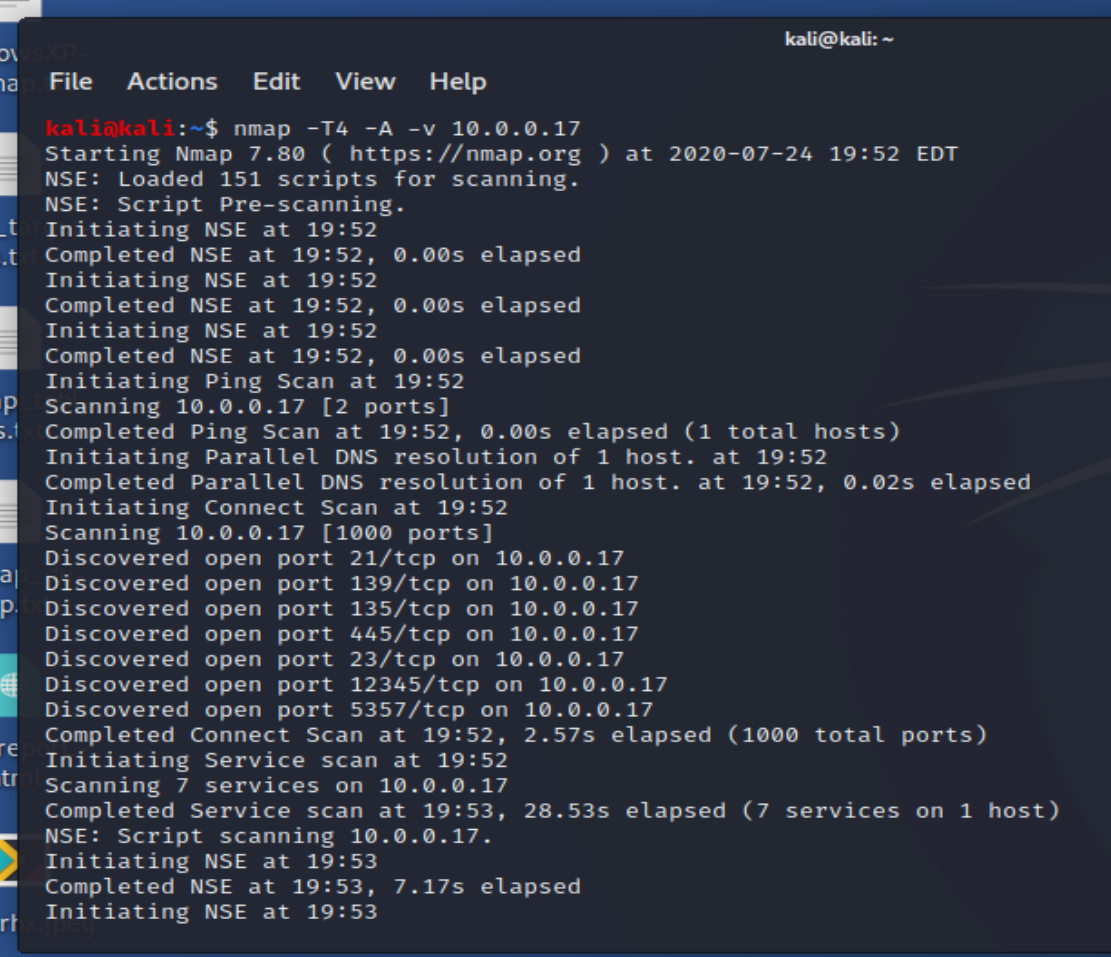


Back on the Windows 10 VM, Valhala Honeypot should have detected and logged that a system had tried to invade it through several network ports including ftp and telnet. There is a save button if the logs need to be saved, otherwise, you can clear them by selecting clear. Next, make sure Valhala Honeypot is still monitoring and head back to the terminal in the Kali system to perform a more invasive Nmap scan.

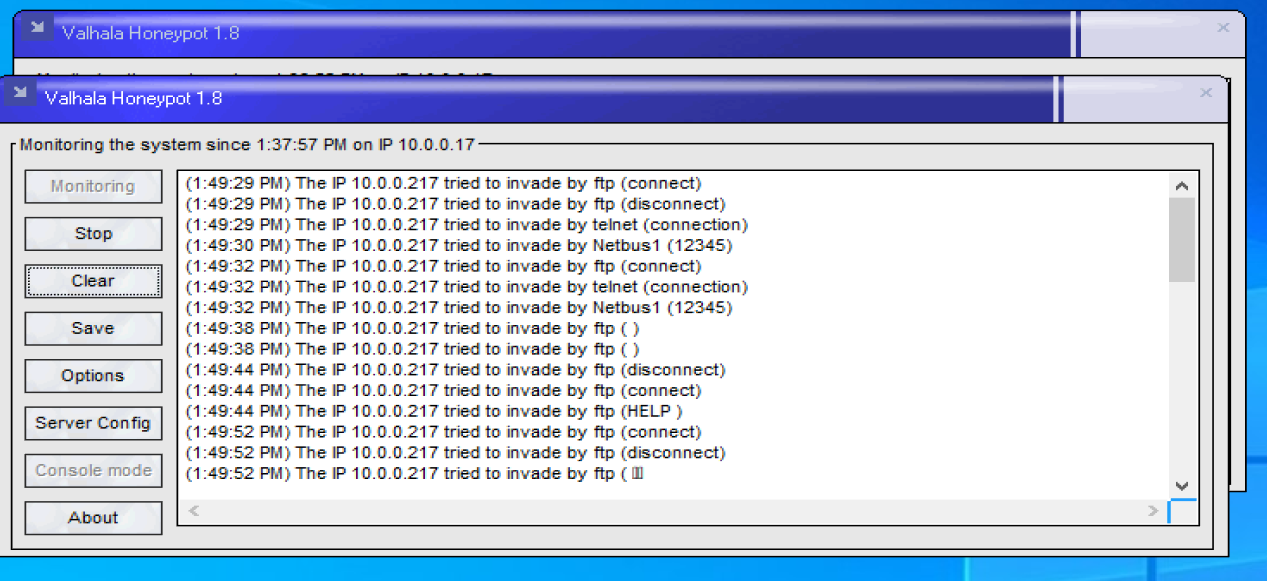
Do an aggressive port scan by using the command:

**nmap -T4 -A -v (“Windows 10 ip address”)**

Example: nmap -T4 -A -v 10.0.0.17



This command is much more detectable but will provide more information about the system.



Valhala Honeypot should again be able to detect that a system tried to invade it using the network ports 21 (FTP) and 23 (Telnet). The honeypot will also show that the invader had connected but was disconnected by the honeypot machine.