Seth Ayers

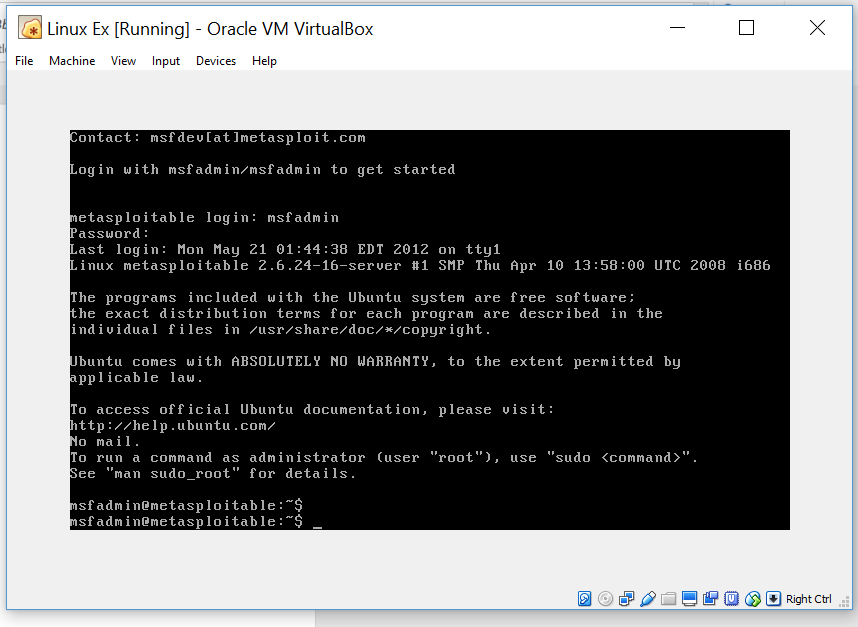
03/07/2018

IT 430 – 02

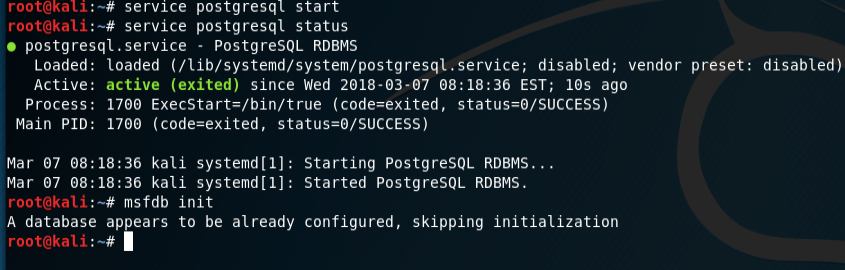
Lab 05 Metasploit Framework

SAyers\_Lab05.docx

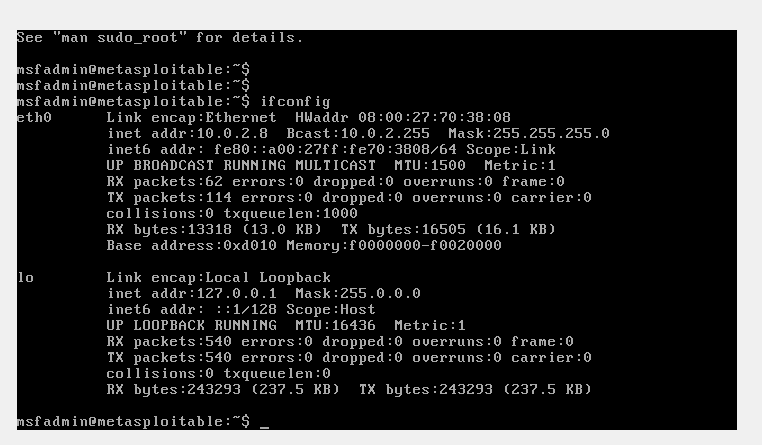
**Assignment 1: Follow the lab instructions.**



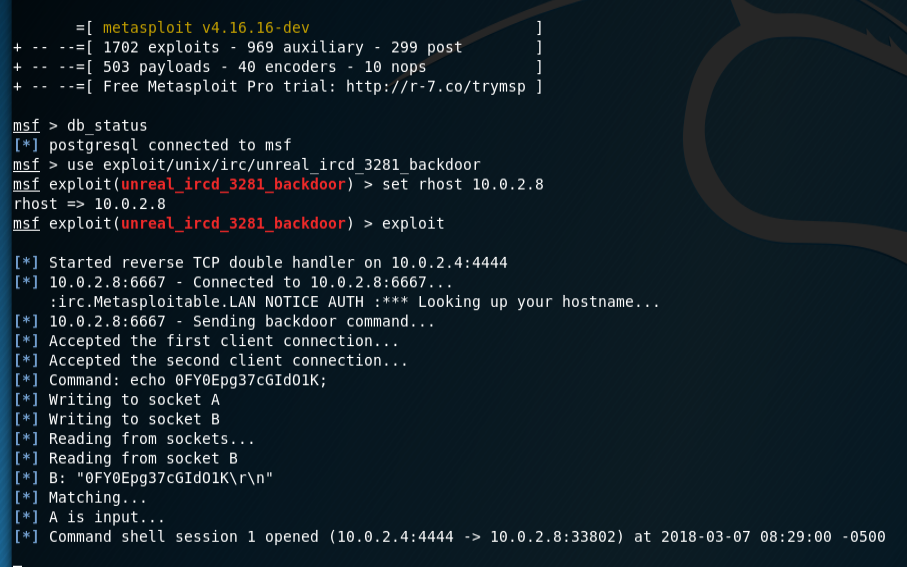
*Environment logon*



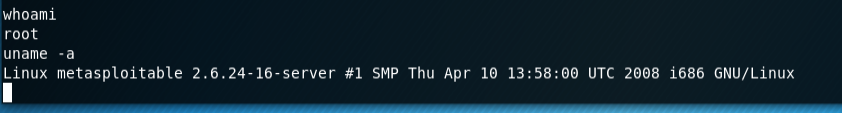
*Postgresql initialization*



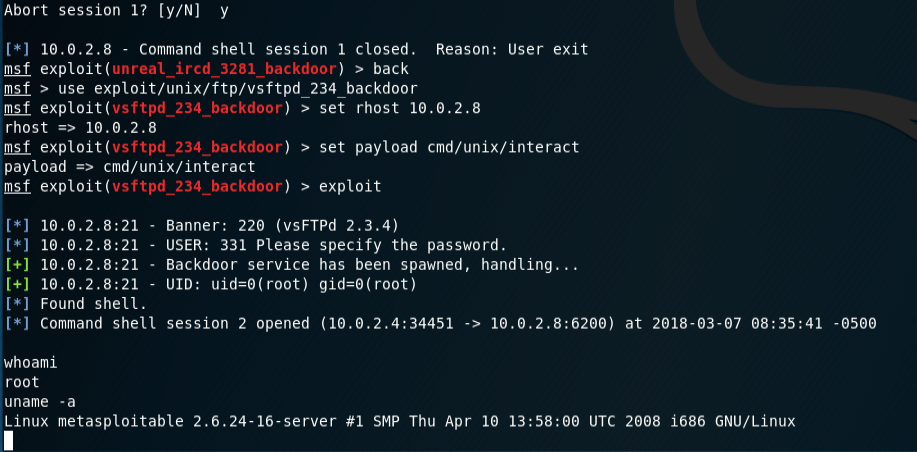
*IP information of Metasploitable2-Linux*



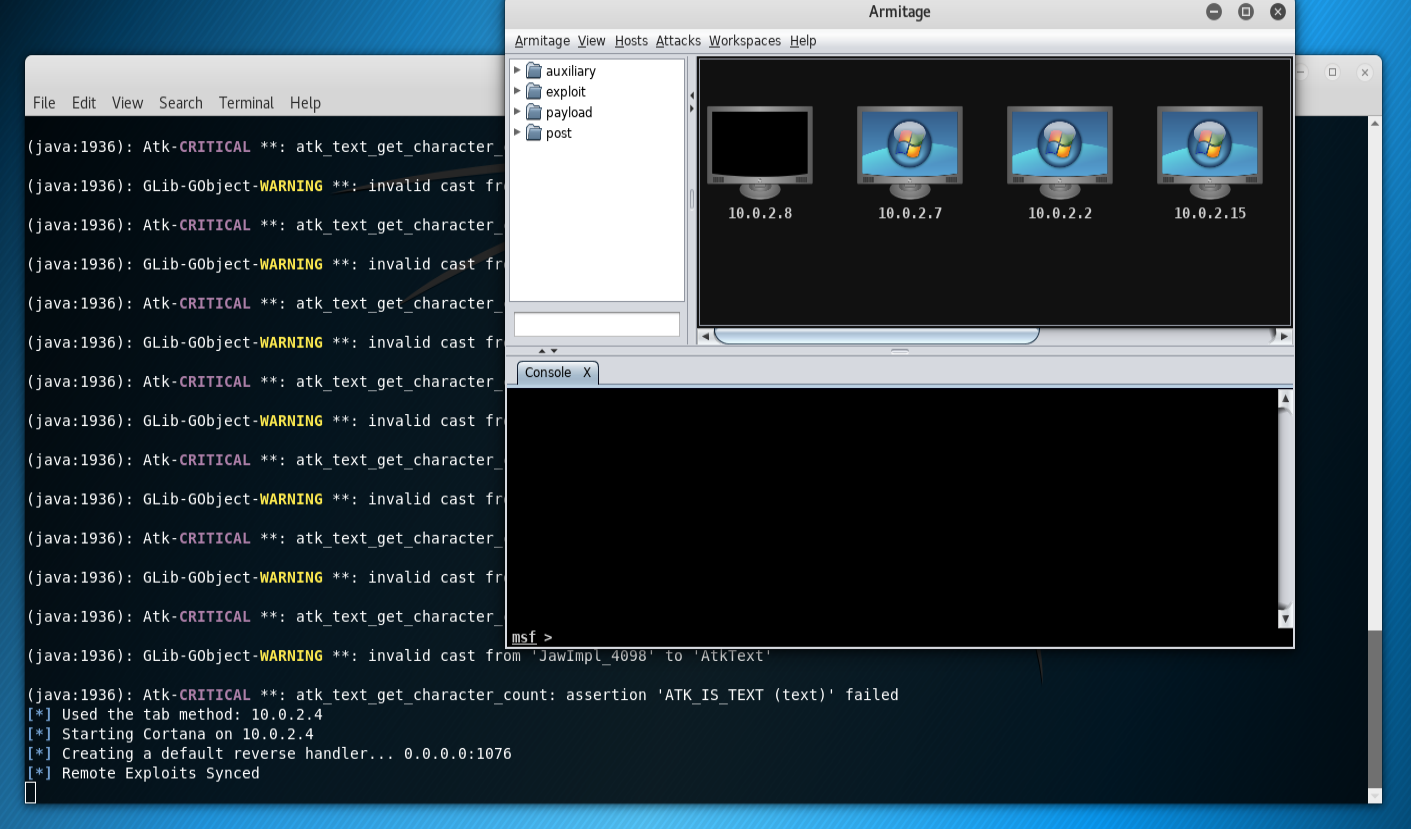
*Execution of unreal\_ircd\_3281\_backdoor exploit*



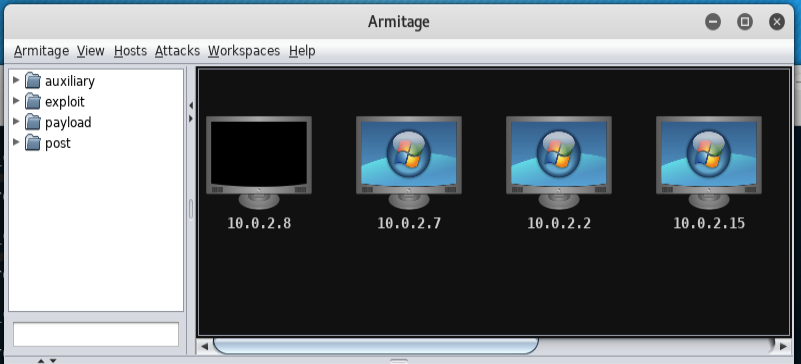
*Confirmation of access*

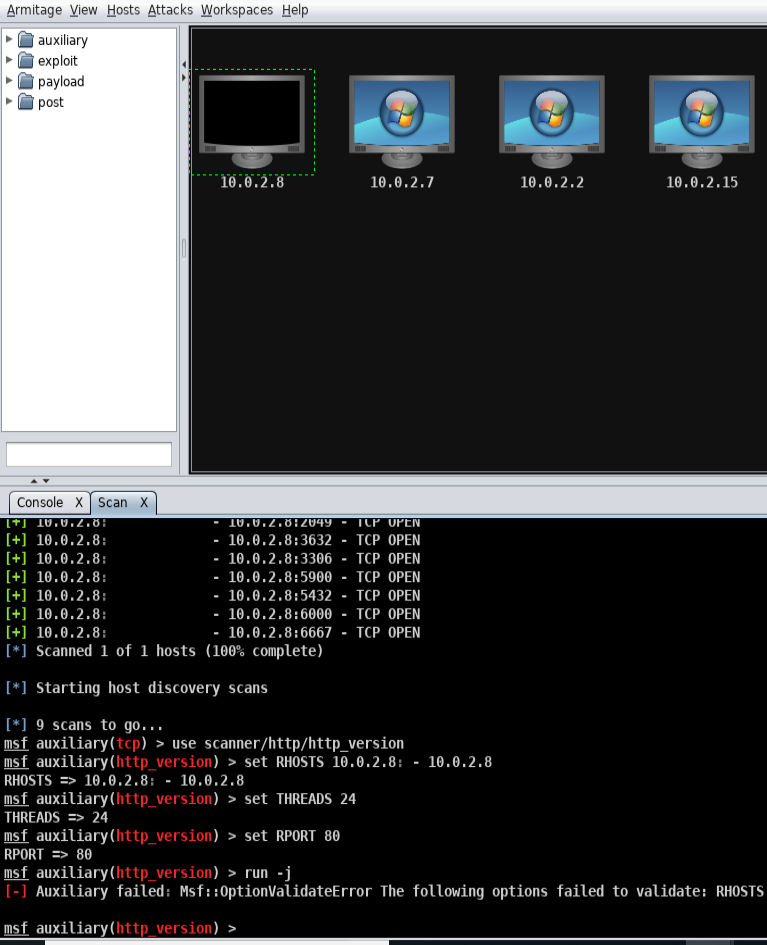


*Execution of vsftpd\_234\_backdoor and confirmation of access*

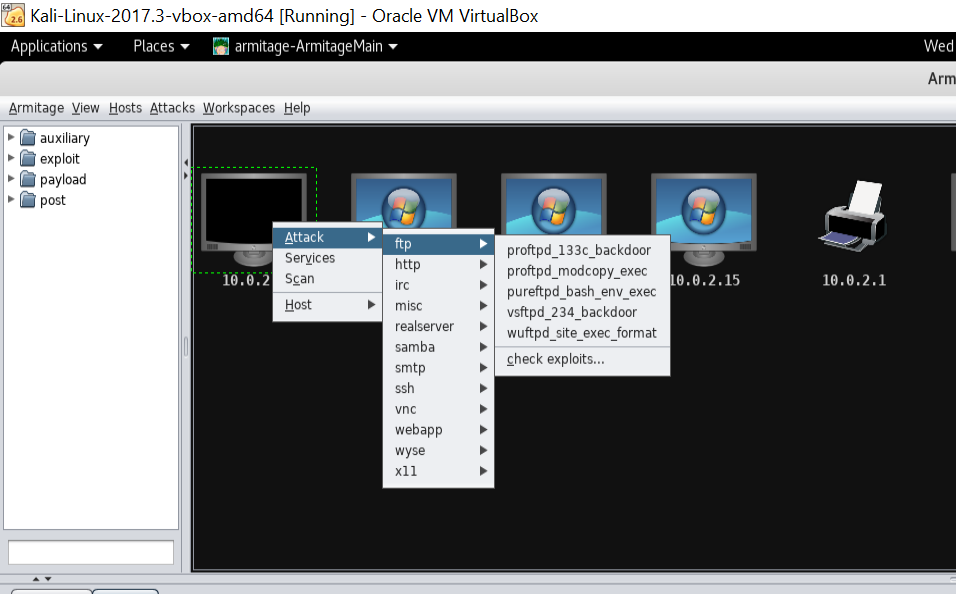


*GUI interface of Armitage, started via Unix*

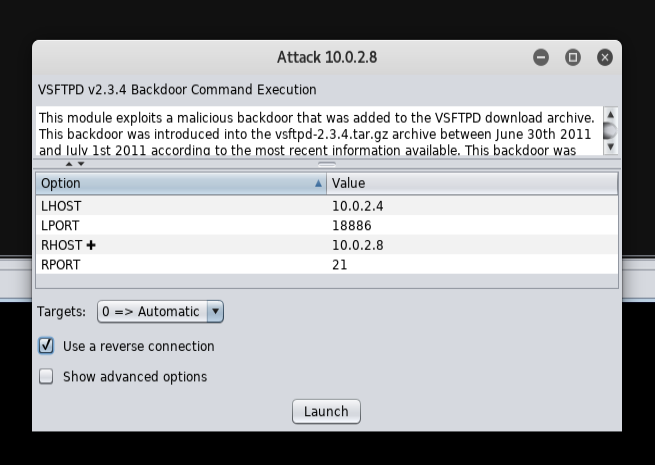


*Metasploitable2-Linux host (10.0.2.8) added to host pool*

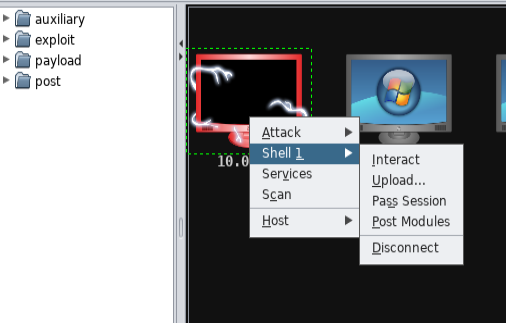
*Scan of host 10.0.2.8*



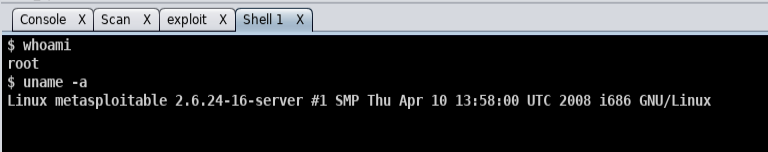
*Attacks found for target host*



*VSFTPD Backdoor explanation and execution options*

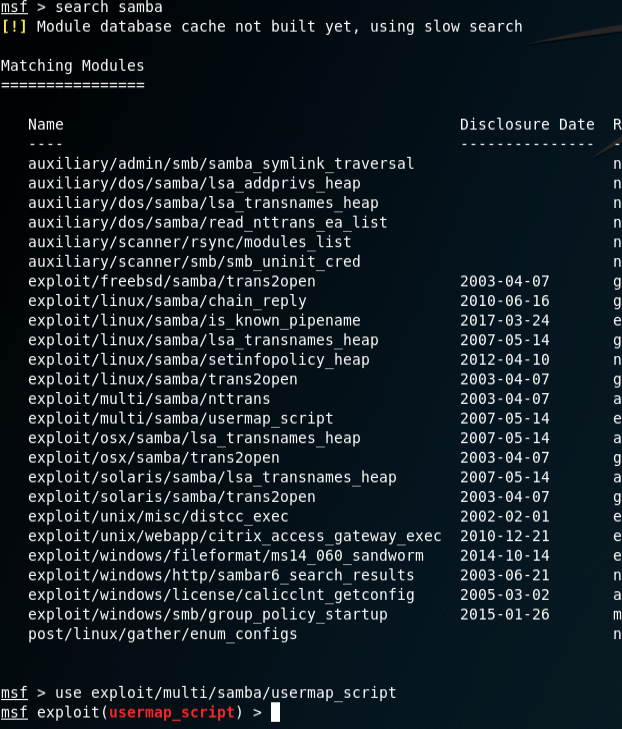


*Interaction with 10.0.2.8 shell*

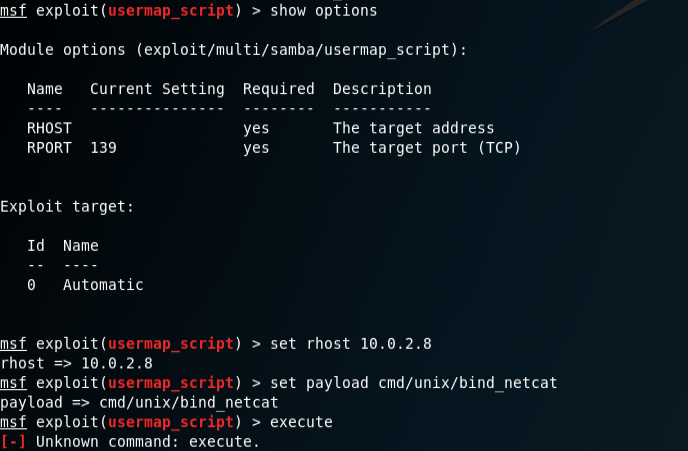


*Connection confirmation of 10.0.2.8*

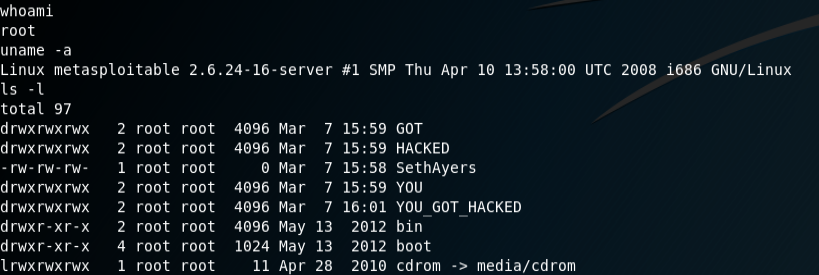
**Part D: Using other exploits**



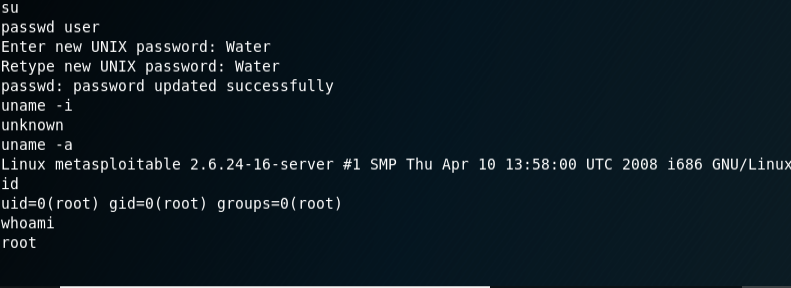
*List of exploits that involve samba (port 445)*



*Options available for username\_script exploit/Setting options*

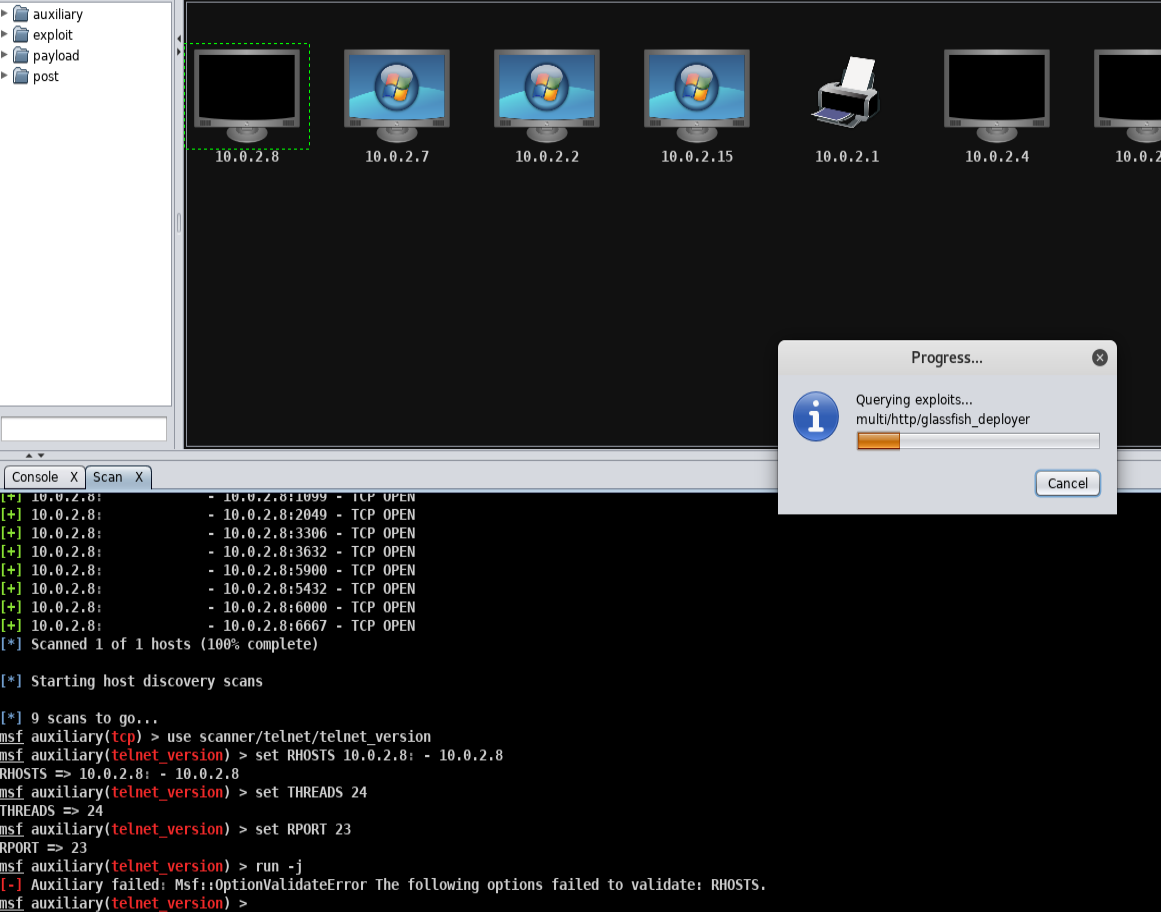


*After gaining access to the shell, I built files and directories*….

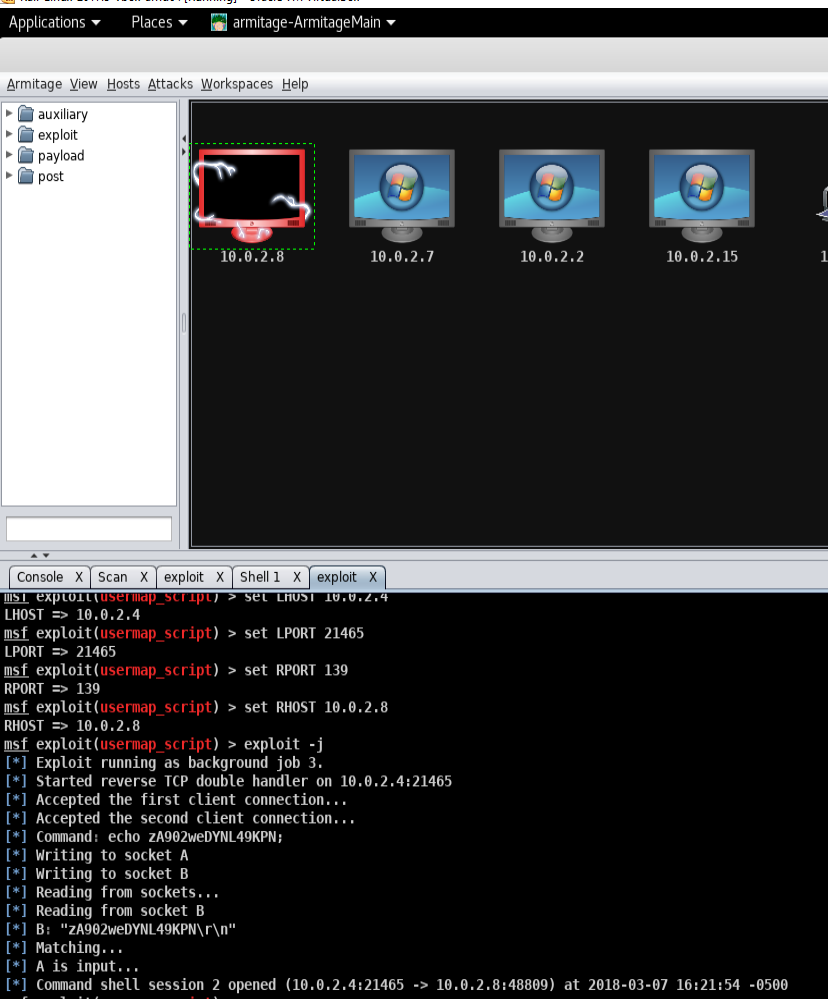


*.. And I also managed to change the root password*

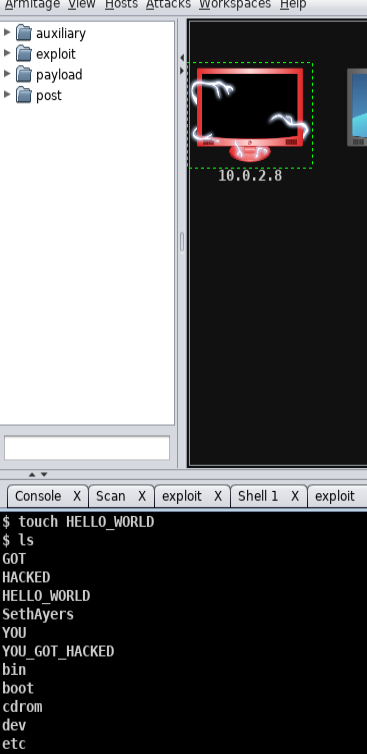
**Armitage:**



*Scanning the 10.0.2.8 host for usable exploits*



*Executing the usermap\_script*



*Confirming root shell access by viewing file/directories previously made in the above steps*

**Part E: Reflections and observations**

Metasploit, at its core, is a powerful pentest tool made to utilize the information gained from various forms of footprinting and reconnaissance. With the reconnaissance information in hand, aggressive Nmap scans can give the user operating system information, patch/version/build information, running services, open ports, and some network topography information (hops, host types). Once this information on a target is gained, a list of known exploits is available that could potentially be used to affect the target system. While a provided list is a nice touch, I feel a security professional should closely examine why the exploits work, specifically the “mechanics” of the attack, rather than relying on pre-compiled scripts that someone else engineered. Knowing the internal working of ports and protocols, as well as studying the script/code of the attack itself, is the line that divides the professionals from the “script kiddies”.

The use of Metasploit should be used with the upmost care, because although accessible to the public, it is an extremely effective hacking/cracking tool. While there are some exploits in the database that are older, and most likely patched on most systems, the database is continuously updated with new exploits once application updates are performed. Respect and integrity must be considered while using a tool such as Metasploit, as the use of it for malicious intent is not only ethically wrong, but very illegal as well.

In terms of the lab, the backdoor exploits preformed were used to gain direct access to the target host’s root account. Through some Unix commands, an attacker could access user accounts, password hashes, sensitive data, install/write malicious scripts, install bot nets, or completely shut the end user out by bricking the OS. After doing some research online, I decided to perform a “username map script” exploit. Firstly, port 445 is highly susceptible to attacks due to being deeply ingrained in operating systems and internal network file sharing (SMB or “Server Message Block”). Typically, port 445 should always be disabled at the last point of the network, going out to the internet. Many commercial service providers do this automatically for their customers, as a default, due to the remote access exploits that can be performed on the host. Regardless, these ports are still left open on some hosts/networks all across the internet and can be found by hackers with NetBIOS worms or manual reconnaissance. In the username map script exploit, remote shell access is granted via a security loophole in SAMBA, where credentials to the user is not required for access.

**Other observations:**

As for my preference between the GUI base Armitage or the Metasploit cmd line, I do prefer Metasploit. This is somewhat based on my bias towards command line operation, specifically Unix, but also the lightweight, responsive feel and quickness of Metasploit itself. If anything, Armitage is a good tool to get familiar with the internal workings of Metasploit, as the console window displays the automated commands, step by step. This feature can be observed to find the “how and why” behind the commands themselves.

Lastly, to answer the question of “Why do we need to assign an internal IP address (i.e., behind NAT) for Metasploitable2-Linux? What will happen if we assign a public IP to it?”. We use the NAT function to completely remove the Metasploitable host from the internet for obvious reasons, that are quite clearly shown in the lab. It’s an environment based on the lack of security patches for learning purposes. To have the host on the open internet is basically inviting a someone to gain access, and in turn, gaining access to our personal networks. This would put our personal network and devices at risk. The host, by no means, should be connected directly to a personal network, ever.