Domain: Offensive Security

Question: Penetrating & Persisting in a Network

What steps would you take to penetrate a network, and what would you do once you've gained access?

When penetrating a Network, the first thing to do is research exposed services and vulnerabilities and go further with exploitation. For Project III, the attack virtual machine (VM) Kali was used to penetrate “Target 1” or the victim's machine. Within the Network, we had an ELK VM, which was used to set up the alerts, and a Capstone VM that was used to test those alerts. The goal was to infiltrate Target 1. A few commands were run in Target 1 to ensure that it forwards logs to Kibana. Target 1 credentials vagrant:tnargav. Escalate to root *sudo -s* and */opt/setup/*

In Kali, the nmap command *nmap -sV 192.168.1.110* was used to expose any open ports. In this case, Target 1 had a few open ports including port 22/tcp ssh and port 80/tcp http. At this point we know that we can ssh into Target 1 and gain unrestricted access as a user. We know the IP for Target 1 and now we need to find user names and their passwords. Since we are targeting a WordPress site, the command wpscan *wpscan --url http://192.168.1.110/wordpress -eu* revealed two users (Michael and Steven). Hydra *hydra -l michael -P /usr/share/john/password.lst ssh://192.168.1.110 -t 4* revealed Michael's weak password as “michael”. Now we have all the necessary information to login as Michael anytime we want. We have a backdoor. By ssh into Target 1 as Michael we found the firsts flags.

In addition, very critical information was found. The file wp-config.php in path /var/www/html had the name of the MySQL database used “wordpress”, the username: “root”, and the password “R@v3nSecurity”. As “Michael” I used command *mysql -u root -pR@v3nSecurity wordpress* to gain access to MySQL, then *show tables;* and *SELECT * FROM wp_users;* The hashed passwords of Michael and Steven were there. Steven’s password was cracked using John the Ripper (steven:pink84), another flag was found and the last flag was inside table wp_posts in My SQL.