**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?

**Answer:**

To reiterate, the question was what steps would I take to penetrate a network, and what would I do once I’ve gained access?

In a recent project, as part of the Red Team, we had to identify and exploit weaknesses and threats within an organization’s network. The network contained 3 virtual machines. The machines were the Kali attack machine, the Capstone victim machine and the Kibana machine which captures all information performed by the Red Team. The goal of infiltrating the victim’s machine is to use all methods that an attacker would use to infiltrate and exploit a system in order to provide an organization with a report of all their vulnerabilities in their network.

To infiltrate the Capstone machine, we first had to retrieve the network configuration, identify the host and ports available on that network. One of the stealthy techniques used for a port scan is the nmap tool to see what services are open.

The port scan identified that port 80 was open for the Capstone machine. From a web browser, we navigated to the IP address and found several files indicating there was a secret folder. While trying to access this folder, we found what login username we would need to use to try to crack its password.

We brute forced the password using the login cracking tool hydra. Once we retrieved the login credentials, we were able to successfully access that secret folder and its contents. The folder contained a file that gave instructions on how to connect to the victim’s machine, Capstone.

In order to log into the victim’s machine, we first had to crack the hash password for the user identified in the file. Then we connected to the victim’s machine via WebDav using the login credentials we just retrieved. From here, we were able to copy a file into the victim’s machine.

A PHP reverse shell payload was created to open up a meterpreter session through Metasploit. Through this session, we were able to maneuver within the system and even download a file.

The issue that we might encounter once we have exploited a network is trying to reconnect back without having to re-exploit into the network. We can use Metasploit’s tools such as the keylogger script to gain information about other user accounts and passwords. Or use Metasploit's metsvc backdoor service to be able to log back into a meterpreter session. There is also Metasploit’s persistence script that even if the victim’s system is rebooted, this will create a meterpreter service.

The techniques used by the Red team to exploit a victim’s machines helps to identify vulnerabilities that can be exploited by attackers for malicious purposes. There is always going to be a situation where not every vulnerability has been identified because attackers will always try to find many techniques and tool, with patience, to break into a system!