OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Extra Credit: Persistent Access

Alexander Kotzian

.

Extra Credit

1. Setup:
    a. Ensure that all three machines are set up and connected within the same network.
    b. Verify that necessary tools like Metasploit and any required payloads are available on Internal Kali.
2. Initial Access:
    a. From Internal Kali, launch the exploit targeting vulnerabilities in the Windows 7 machine.
    b. Gain a reverse shell connection to the target Windows 7 machine.
3. Payload Upload:
    a. Once the reverse shell connection is established, proceed to upload the payload onto the Windows 7 system.
    b. Craft the payload to establish a covert connection with External Kali upon the next login attempt by the user.
4. Scheduling Tasks:
    a. Utilize the Windows Task Scheduler to create a scheduled task on the compromised system.
    b. Configure the task to execute the uploaded payload upon user login. ensuring persistent access to the system for future interactions.
5. Testing:
    a. Restart the Windows 7 machine to simulate a logout/login event.
    b. Verify that the scheduled task successfully executes the payload and establishes a connection with External Kali

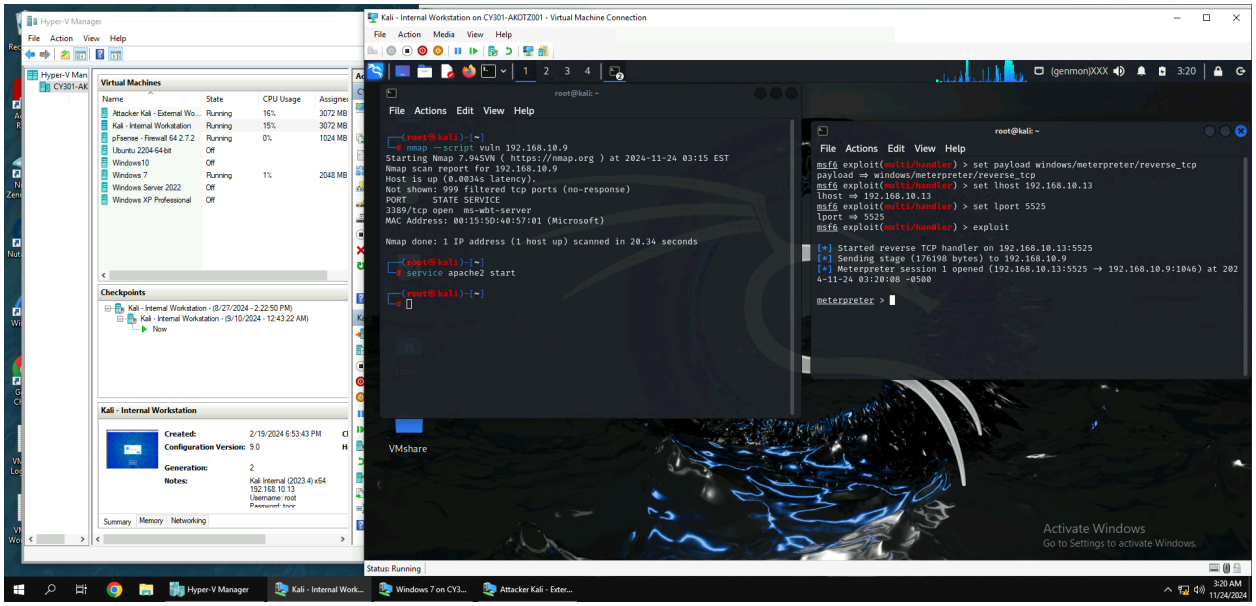

Figure 1

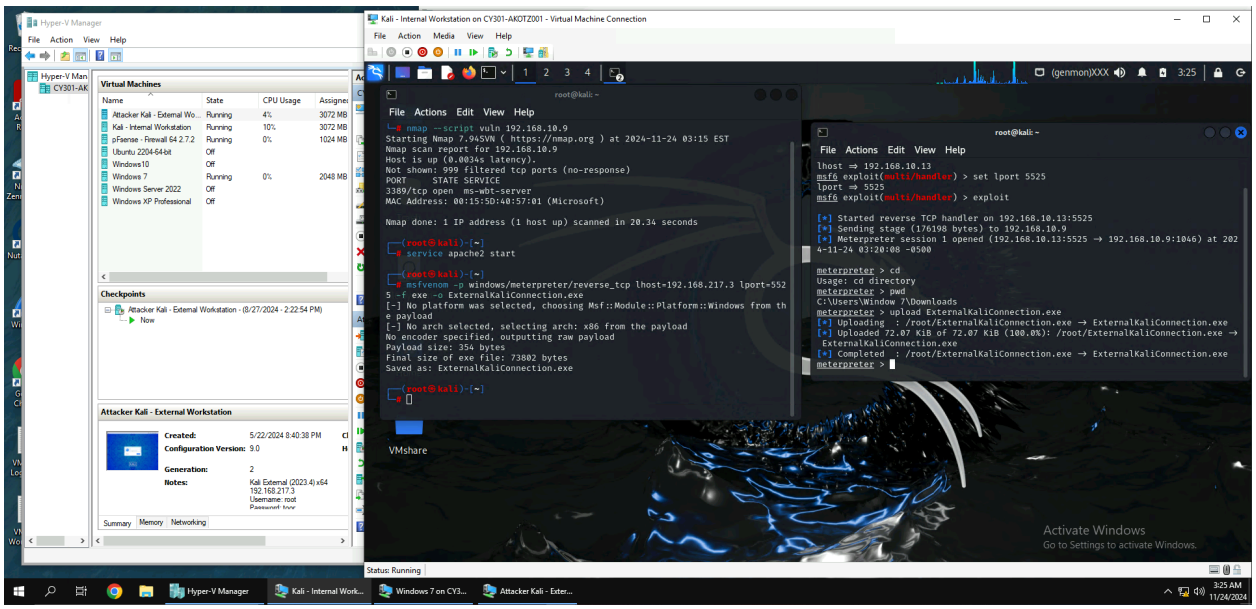

Figure 2

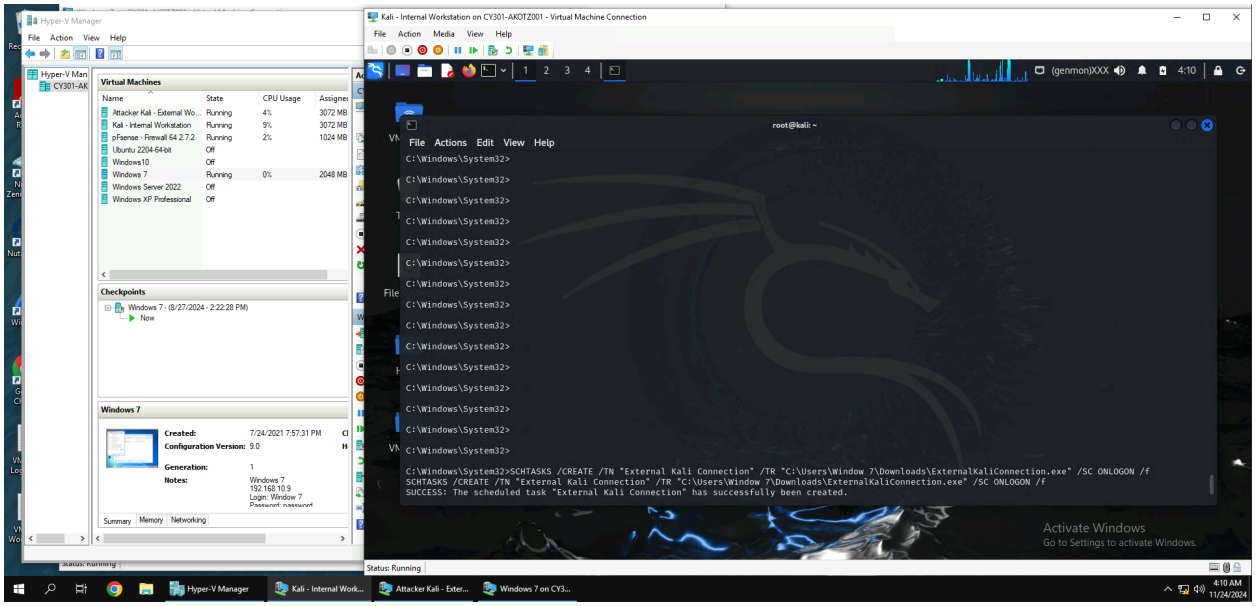

Figure 3

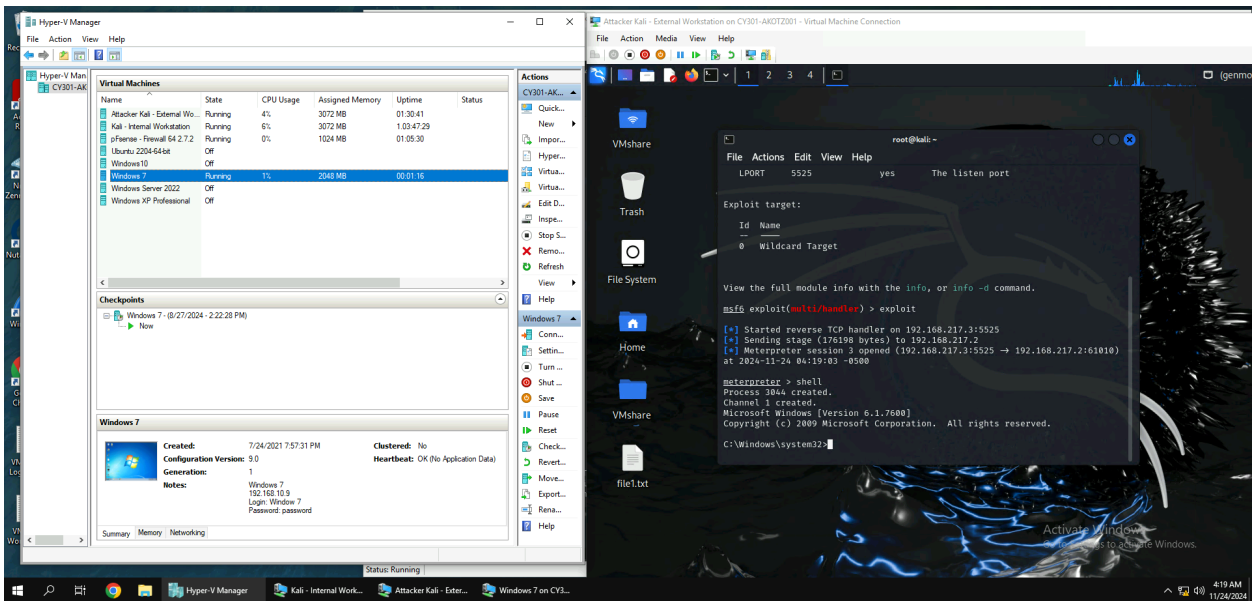

Figure 4

Figure 1 shows that all needed VMs are running, and that metasploit is installed on the Internal Kali VM. Additionally, it shows that I used the payload method to create a reverse shell connection to the Windows 7 VM, this is because the nmap scan did not result in any vulnerabilities being detected on Windows 7 device. Figure 2 shows the creation of the External Kali Connection payload, as well as it being uploaded to the Windows 7 VM. Figure 3 shows a successful scheduled task on Windows via reverse shell connection, which in turn should activate upon every log in to the Windows 7 VM. Figure 4 shows a successful logon initiated payload by a successful reverse shell connection from the External Kali VM to the Windows 7 VM.

Your lab report MUST satisfy the following Requirements. Otherwise, you will lose points.

- R1 - Include a cover page with your UIN and name.
- R2 - Align your screenshot(s) with the task ID and description.
- R3 – Use “Snipping tool” or other tools, such as “Snippets”, to take screenshot. MacOS user can follow this post to take screenshots.
- R4 - Include the running VMs (1), system timestamp (2) and session information (3) in every single screenshot.
- R5 - Explain your step(s).