Remote Access Keylogger Installation – Meterpreter

.mp4 Video Tutorial

Remote Access Keylogger using Meterpreter.mp4

If .mp4 file is unavailable access via:
https://drive.google.com/drive/folders/1MaKs7MrtT7RwgnXkoHtAZVh44E29GqUV?usp=sharing

Question 1

a. **Task overview.**
In this task I first exploited a vulnerability in a Windows XP VM to gain access and open 'meterpreter' software which is a part of the Metasploit framework. Through this I was able to remotely open a keylogger malware which allowed me to discretely monitor all keystrokes input in the victim's system.

b. **Discuss why this task is awesome and how you showed independence, professionalism, and ambition to complete it**
I've been particularly interested in the way keylogger malwares operate since they were briefly mentioned in the earlier weeks' lectures. Thus far, we haven't looked particularly deep into keyloggers outside of their overall purpose. The previous distinction task provided a great introduction to the Metasploit framework which I was then able to further research through this task. I was able to not only further explore some of the commands and exploits available within the Metasploit framework but also how it can be used to interact with other operating systems (Windows XP in this case). I was especially surprised with not only how quickly a system can be compromised but also how quietly/discretely it can be done. In this instance there was no indication whatsoever on the victim's computer that the system had at all been compromised or that the keylogger had been activated.

Additionally, this task displayed both ambition and independence. Firstly, this task was something I'd been hoping would be covered in the course and this assignment gave me the opportunity to explore an area of cyber security that I found particularly interesting. It further displayed independence as all research for the task was undertaken independently. Furthermore, through researching this task I was introduced to the topic of pentesting and what this job typically involves which I found especially interesting. I also displayed professionalism throughout the task by completing it within a simulated environment (Windows VM) which would cause no potential harm or damage to an unsuspecting victim.

c. **A brief reflection about what you learned and how you found the task (reflection)** Before undertaking this task, I assumed all forms of hacking where especially complex and required extensive knowledge and a profound understanding of computers to complete. While of course the user must have a foundational knowledge and pre-existing skillset to realistically attempt the task, the amount of readily available information and software available to assist the user gave me a better insight into how easily computer systems can be exploited and consequently the dire need for computer security. This task also gave me a practical understanding of the need for ethical hackers or pentesters outside of a typical textbook knowledge. Without pentesters to explore the potential vulnerabilities and exploits in

computer systems, those exploits are otherwise left to be discovered by adversaries with malicious intent; much the way a compromised password is not discovered until it is too late. Much like the previous distinction task, I initially found it to be quite overwhelming, thinking I wasn't equipped to complete something which could be applied to a real-world situation. I had originally planned on doing the research task as I felt it was something I was more equipped to handle however decided against it as I wanted to push myself and further explore the field of cyber security in a practical manner. Ultimately, this task stressed the importance of computer security and how vulnerable our systems are if we don't take the necessary precautions to protect them. This was my favourite task this far as I really felt as if I was getting a better insight into my desired field.