Team 5
Group Proposal

Backdoor Man In the Middle Attack Proposal

We are proposing a backdoor man in the middle attack. The basic idea is that we will intercept network traffic and then use it to set up a backdoor on the target machine. Initially we will use a linux virtual machine as our target. Intercepting traffic will be done by setting up a wifi access point on our machine. Once we have intercepted traffic we will redirect the user and trick them into downloading our backdoor code or enabling a backdoor with a command. Alternatively we will look into methods of injecting our code into the intercepted traffic without the target's knowledge. Finally we will explore various ways that we can protect ourselves from backdoor and networked man in the middle attacks.

Links:

- Intercepting Traffic
  - https://hackernoon.com/a-hacker-intercepted-your-wifi-traffic-stole-your-contacts-passwords-financial-data-heres-how-4fc0df9ff152
  - https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/
- Tricking Users
  - https://www.thatsnonsense.com/how-websites-can-trick-you-into-downloading-malware/
- Backdoors
  - https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/
  - https://medium.com/@airman604/9-ways-to-backdoor-a-linux-box-f5f83bae5a3c
  - https://www.abusix.com/blog/how-hackers-access-networks-using-backdoors
  - https://dev.to/tman540/simple-remote-backdoor-with-python-33a0
- Protecting Against Attacks
  - https://www.malwarebytes.com/backdoor/#how-can-i-protect-against-backdoors